Act CIII of 2023

on the digital State and certain rules for the provision of digital services

With a view to transitioning the relations between the State and society into the digital space and establishing modern digital governmental platforms and services, the National Assembly, recognising that the development of information and communication technologies leads to a radical transformation of our lives, adopts the following Act on the basis of Article XXVI of the Fundamental Law:

FIRST PART

GENERAL PROVISIONS

Chapter I

INTRODUCTORY PROVISIONS

1. Purpose of the Act

Section 1 The purpose of the Act is to establish digital citizenship and, in this context, to lay user-friendly foundations for administration and service provision in the digital space. In order to ensure simple, convenient and efficient service provision, this Act shall provide for the following in the digital space:

a) possibility of using comprehensive digital services operating on uniform foundations, in particular identification and signature, secure electronic communication and document management as well as online payment systems relating to services;

b) optimisation and digitalisation of services provided by the State to society;

c) primacy of administration through mobile phones and other portable devices capable of establishing digital data connection;

d) uniform framework for digital administration at organisations required to provide, or undertaking the provision of, a digital service;

e) using data available in state registers to improve the quality of public services, as well as cooperation among state organs; and

f) digitalisation of civil law relationships.

2. Scope of the Act

Section 2 (1) The scope of the Act shall cover the content of digital services specified in an Act or a government decree and their use in the digital space.

(2) The scope of the Act shall cover

a) natural persons, economic operators and other legal entities using digital services;

b) organs required to provide digital services;

c) organisations required to ensure digital services; and

d) legal entities voluntarily undertaking the provision of a digital service

[organisations referred to in points b) to d) hereinafter jointly "digital service provider"]

(3) The scope of this Act shall, for the implementation of digital services, cover the following:

a) providers of supporting services within the meaning of this Act;

b) the organ designated by the Government for providing the digital framework application, digital framework services, and life-event-based services as well as the digital citizenship service provider.

(4) For the purpose of the implementation of digital citizenship, the primary objective of the service provider referred to in paragraph (3) b) shall be to ensure the possibility of using the service via portable devices, to provide the related supporting services and to perform data processing operations that comply with the requirements laid down in sections 3 (4) and 5 (1) and (2).

(5) In line with this Act, an Act shall provide for

a) the right to informational self-determination and the freedom of information;

b) the cybersecurity of Hungary; and

c) the system for the utilisation of national data assets and certain services.

3. Principles and fundamental provisions of the Act

Section 3 (1) This Act shall ensure the user-friendly and client-centric provision and use of digital services.

(2) Digital service providers, the digital citizenship service provider, and the supporting service provider shall design digital services and the required system processes primarily with regard to the individual life events of the user.

(3) For the purpose of uniform access to administration in the digital space, the State shall provide a unique and permanent digital identifier in accordance with Article XXVI (2) of the Fundamental Law.

(4) The identifier referred to in paragraph (3) shall ensure that services provided in the digital space may be accessed easily through a generally usable identifier, and that data and records required for the provision of such services, that are held in specific registers or by specific organs, are made available in an automated manner.

(5) Unless otherwise provided in an Act or a government decree, digital citizenship services, in particular the framework application and the framework services, shall be free of charge for users. The fact that the digital service is free of charge shall be without prejudice to any payment obligations arising from matters to be administered through the service.

(6) The digital services shall be primarily accessible through the digital citizenship framework application.

(7) The national digital identity wallet shall be a service developed for a mobile application that is suitable for identification and verification of other data and attributes both in the digital space and during in-person interactions.

(8) Digital citizenship services may also be used in the course of the provision of public and other services. The digital services shall be provided to users by the organisations specified in this Act; an economic operator may voluntarily undertake the provision of certain digital services also on the basis of a licence.

Section 4 (1) In the digital space, a user profile based on a digital citizen identifier shall serve as the primary means of communication with the State.

(2) The holder of a user profile shall decide whether to use the services provided by digital citizenship. The user profile shall be activated in order to use the services provided by digital citizenship.

(3) The holder of a user profile may decide not to activate or to deactivate the user profile.

Section 5 (1) Digital citizenship shall be based on data processed in state registers. Within the framework of digital citizenship, all state registers and sectoral systems shall cooperate in a coordinated manner in accordance with the provisions of this Act with a view to ensuring digital citizenship services and services provided under an aggregate service, and shall automatically provide data to the extent necessary for digital service provision.

(1a) The digital citizenship service provider and the provider of a life-event-based service shall be exempt from paying administrative service fee and other fees for data provided from the registers and sectoral systems referred to in paragraph (1) in the context of the performance of their public duties specified in this Act and the decrees issued on the basis of authorisation by this Act.

(1b) For the purpose of service provision, the digital citizenship service provider, the provider of a life-event-based service, and the provider of supporting services may use framework and supporting services free of charge.

(1c) An aggregate service shall qualify as an authentic source within the meaning of Article 3, point 47 of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (hereinafter the "eIDAS Regulation").

(1d) If required by law, data requests from certain registers and data queries may be carried out also through an aggregate service.

(2) A user shall not be required to repeatedly provide data that is available in the digital space.

(3) The State may use data generated or appearing in the digital space that are not suitable for unique identification for the purpose of improving existing digital services, introducing new digital services and providing a basis for public administration decision-making.

(4) In order to support the competitiveness of undertakings, the legal entities referred to in section 2 (2) c) and d) shall use digital identification solutions, electronic signatures, electronic seals and time stamps, storage services and other supporting services in accordance with the provisions of the law.

(5) The protection of personal data and the security of electronic information systems shall be ensured in the digital space.

(6) All users shall have the right to information, and to be informed, relating to digital services. All organisations providing a service under this Act shall ensure that this right is respected, in particular through the publication of easily understandable information materials, the operation of a customer service, and the provision of informative content facilitating the use of the services.

(7) When providing digital services, efforts shall be made to ensure access to the services without any discrimination based on disability.

(8) Digital citizenship services shall be designed to be portable-device- and platform-independent and to be accessible to the widest possible range of users.

Section 6 (1) In Hungary, a user shall be entitled to administer matters with a digital service provider by digital means in accordance with the provisions of this Act.

(2) With regard to persons detained in the course of enforcing a penalty, measure, or coercive measure, the right provided for under paragraph (1) may be restricted in an Act with a view to preserving the order of enforcement, maintaining the security of detention, and securing the success of a criminal proceeding If a person detained would be required to use a digital service, he shall be relieved of such an obligation.

(3) The legal effect of a submission provided digitally shall not be denied solely on the grounds that it is in an electronic form.

(4) An organ required to provide a digital service shall operate in a fully digital manner all internal functions and processes that are required for the functioning of its digital services and for communicating with counterparts involved in the administration of matters, and shall provide the necessary electronic information systems.

Section 7 (1) Unless otherwise provided in an Act or a government decree, digital services shall be established and operated in the digital space.

(2) New digitals services and their legal and technical environment shall be established in accordance with the principles of digital citizenship.

(3) The Government shall set out in a decree the date from which all services that affect a broad range of citizens and undertakings and determine their everyday life and activities shall be accessible exclusively in the digital space.

4. Interpretative provisions

Section 8 For the purposes of this Act:

1. *aggregate service* means an integrated service based on data processed in state registers and other electronic information systems that is provided by the digital citizenship service provider using the data processed by the organisations connected to the service;

1a. *electronic registered delivery service* means the term as defined in Article 3, point (36) of the eIDAS Regulation;

2. *attribute* means the term as defined in Article 3, point (43) of the eIDAS Regulation;

3. *internal register* means a register kept for the sole purpose of serving the objectives, tasks and supervision activities of the organ keeping that register, and that is not intended to transfer data to third parties and does not qualify as a source of information for third parties;

4. *trust service* means a service as defined in Article 3, point (16) of the eIDAS Regulation;

5. *trust service policy* means a set of rules in which a trust service provider, relying party, or another person lays down the terms of using a trust service for groups of relying parties with certain common security requirements or for specific applications;

6. *trust service client* means a person who enters into a service contract with a trust service provider;

7. *trust service provider* means a trust service provider as defined in Article 3, point (19) of the eIDAS Regulation;

8. *digital citizenship* means the right of citizens to administer matters and use services digitally;

9. *digital citizen identifier* means a sequence of digits generated by a mathematical method that does not refer to any sensitive data and, as a unique and permanent identifier, unambiguously identifies the citizen in the digital space;

10. *digital citizenship register* means client registration records established by this Act;

11. *national digital identity wallet* means a digital service which allows the user to store identification data, including person identification data and identity-related electronic certificates, to make such data available upon request, and to ensure electronic identification, and electronic signature and electronic seal placement;

12. *digital service* means a matter falling within the functions and powers of a digital service provider and a service providing, in accordance with this Act, administration relating to a service to be provided by the digital service provider pursuant to the law, and the cooperative system thereof;

13. *digital space* means the environment for the conduct of state, social and economic interactions electronically, without requiring physical presence;

14. *electronic identification* means the process described in Article 3, point (1) of the eIDAS Regulation;

15. *simple electronic signature* means a signature as defined in Article 3, point (10) of the eIDAS Regulation that does not meet the requirements set out in Article 3, points (11) and (12) of the eIDAS Regulation;

15a. *electronic attestation of attributes* means an attestation as defined in Article 3, point (44) of the eIDAS Regulation;

16. *electronic seal* means a seal as defined in Article 3, point (25) of the eIDAS Regulation;

17. *electronic time stamp* means a time stamp as defined in Article 3, point (33) of the eIDAS Regulation;

18. *life event* means a matter or a group of matters that can be organised around an event typically occurring throughout the life of a natural person, with the proviso that a single matter may relate to more than one life event;

19. *validation data* means data as defined in Article 3, point (40) of the eIDAS Regulation;

20. *European Digital Identity Wallet* means a means as defined in Article 3, point (42) of the eIDAS Regulation;

21. *user* means a natural person or other legal entity involved in a matter falling within the competence of a digital service provider as a client, party or subject of the proceeding, other participant in the procedure, person using the service, or the representative thereof, except for a digital service provider and a member or employee of a digital service provider acting in the matter, as well as, for the purposes of PART SIX, the natural or legal person as defined in Article 3, point (5a) of the eIDAS Regulation;

22. *user profile* means a digital account required for activities in the digital space that is provided on the basis of the digital citizen identifier and contains the data of the digital citizen stored in a state register and the statements made by the digital citizen;

23. *advanced electronic signature* means a signature as defined in Article 3, point (11) of the eIDAS Regulation;

24. *economic operator* means an economic operator, as defined in the Code of Civil Procedure, with a registered office in Hungary, with the reservation that, for the purposes of this Act,

a) an association or foundation without a tax number shall not be considered an economic operator;

b) an association, foundation or ecclesiastical legal person with a tax number shall be considered an economic operator.

25. *authentication policy* means a trust service policy concerning certificates issued as part of a trust service;

26. *information transmission* means the transmission and receipt of information among cooperating organs;

27. *information transmission service* means a service as part of which a cooperating organ transmits data or records to another cooperating organ by means of information transmission;

28. *source of information* means a legal entity at which the information is available;

29. *applicable trust service requirements* means the requirements specified in the eIDAS Regulation, its EU implementing acts , this Act, laws adopted on the basis of authorisation by this Act, the service policies and trust service policies of the trust service provider, and decisions passed by the trust service supervisory body regarding the trust service provider;

30. *legal representative* means, unless otherwise provided by law, an attorney-at-law, law firm, or registered in-house legal counsel acting on behalf of the user;

31. *framework application* means a mobile application designed and developed, by or on behalf of the service provider designated by the Government, that is made available to the public for the purpose of using digital citizenship services;

32. *government communications service* means an electronic communications service provided to users specified by law through an electronic communications network that is specified by law and qualifies as a government network under the Act on electronic communications;

33. *central state service* means an IT, network, and infrastructure service provided as a central service other than a regulated electronic administration service provided as a mandatory government service or a central electronic administration service, that the State provides to market participants through a designated central service provider;

33a. *public sector body* means a body as defined in Article 2, point (6) of Regulation (EU) 2024/903 of the European Parliament and of the Council, an organ required to provide a digital service within the meaning of section 9 (2), and an organisation required to ensure a digital service within the meaning of section 80 (1) a) to e), g) and h);

34. *hash* means a string of bits of specified length linked to an electronic document, which is generated using a procedure (hashing procedure) that meets, at the time of generating the string, all the requirements laid down in the implementing decree of this Act;

35. *classified data* means classified data as defined in the Act on the protection of classified data;

36. *qualified trust service* means a service as defined in Article 3, point (17) of the eIDAS Regulation;

37. *qualified trust service provider* means a service as defined in Article 3, point (20) of the eIDAS Regulation;

38. *qualified electronic signature* means a signature as defined in Article 3, point (12) of the eIDAS Regulation;

39. *central state service provided to market participants* means an IT, network or infrastructure service provided by the State that is delivered, on a market basis, by the service provider designated in a decree of the Government to provide an IT, network or infrastructure public service for a purpose other than public duty performance, in the same manner as the original public service, with the variations specified in a decree of the Government as regards technical content;

40. *role* means a characteristic or capacity associated with a natural person as specified in a decree of the Government, including in particular an office, job, position, post, qualification, and entitlement;

41. *role register* means an electronic register attesting roles in accordance with the requirements laid down in a law;

42. *role certificate* means a certificate issued by a role certification provider that is capable of attesting, with respect to a natural person, that the person concerned holds the certified role specified in the role certificate at the time of attaching the electronic signature to the document;

43. *service policy* means a statement made by a trust service provider regarding the detailed procedural or other operational requirements applied concerning the provision of certain trust services;

44. *service contract* means a contract concluded between a trust service provider and a trust service client, either by acceptance of standard contract terms or individually, establishing the conditions for providing and using a trust service;

45. *certificate subject* means a person whose identity or characteristic is certified by a trust service provider in a certificate, including in particular the signatory of a certificate for electronic signature;

46. *certificate* means a certificate for electronic signature, a certificate for electronic seal, a certificate for website authentication, or an electronic attestation issued by a service provider as part of a trust service, which contains the validation data relating to the certificate and all related data required for using the certificate, and which electronic document is reliably protected against forgery using technology available at the time of issuance and during its validity period;

47. *supporting service* means a regulated electronic administration service and a central electronic administration service within the meaning of this Act;

48. *business administration event* means a matter or a group of matters that can be organised around an event typically occurring throughout the operation of an economic operator, with the proviso that a single matter may relate to more than one business administration event.

PART TWO

DIGITAL CITIZENSHIP

5. Digital service providers

Section 9 (1) The organisations referred to in paragraphs (2) and (3) shall provide the digital services falling within their functions and powers to users in the digital space in accordance with the provisions of this Part and Parts Three and Five.

(2) The organs required to provide a digital service shall be the following:

a) state administration organs;

b) local governments;

c) any other legal entity authorised by an Act or a government decree to exercise public administrative powers;

d) the National Office for the Judiciary and the court;

e) the Commissioner for Fundamental Rights;

f) the prosecution service;

g) notaries;

h) bailiffs and independent bailiffs' offices;

i) statutory professional bodies other than wine communities; and

j) legal entities performing a public duty or providing a public service that are required, by an Act or a government decree, to provide a digital service within the meaning of this Act.

(3) The organisations referred to in Part Five shall be the organisations required to ensure a digital service.

(4) A legal entity voluntarily undertaking to provide a digital service may voluntarily undertake to provide, specific digital services subject to permission of the digital services supervisory authority. The permit shall be granted subject to the following conditions:

a) ensuring compliance with the cybersecurity requirements set out in the Act on the cybersecurity of Hungary, and conducting a cybersecurity audit;

b) furthermore,

ba) registration by the digital citizenship service provider, by means of electronic communication;

bb) acceptance of service conditions set out by the digital citizenship service provider;

bc) compliance with technical requirements set out by the digital citizenship service provider;

bd) payment of administrative service fee to the digital citizenship service provider.

(4a) In addition to the conditions set out in paragraph (4), a government decree may set out further admission conditions.

(4b) A legal entity voluntarily undertaking to provide a digital service shall continuously ensure compliance throughout the full period of service provision with the requirements for the permit referred to in paragraph (4).

(4c) A legal entity voluntarily undertaking to provide a digital service may engage an economic operator included in the register maintained by the Supervisory Authority of Regulatory Affairs (hereinafter the "SARA") to facilitate preparation for digital service provision (hereinafter the "integrator").

(4d) SARA shall maintain a register of integrators with the expertise and meeting the infrastructural requirements necessary for the performance of the tasks as specified in decree of the Government, in accordance with the detailed provisions set out in a decree by the president of SARA.

(4e) The register referred to in paragraph (4d) shall contain the following:

a) name and seat of the integrator, and natural identification data, phone number and electronic mailing address of its designated contact person;

b) identifier of the integrator, received upon registration;

c) documents substantiating compliance with the requirements set out in a decree of the Government decree;

d) further data, not qualifying as personal data, specified in a decree by the president of SARA.

(5) The provisions of this Act shall apply to an organ referred to in paragraph (2) also in the context of matters relating to its functional operation.

6. Digital citizen identifier and digital citizenship register

Section 10 (1) All persons falling within the scope of the register of personal data and addresses shall be entitled to digital citizenship and digital citizen identifier, even absent a relevant request.

(2) The digital citizen identifier shall be generated upon entry into the digital citizenship register (for the purposes of this subtitle, hereinafter the "register").

(3) No official verification card need be issued for the purpose of certifying the digital citizen identifier.

(4) A digital service provider is required to ensure, through the service *eAzonosítás* (eIdentification), the option of identification by means of digital citizen identifier.

(5) A user, when using a digital service within the meaning of this Act or administering matters electronically, shall not be required to use an identification code other than the digital citizen identifier. If a digital service provider connected to the services of a data link register regulated by the Act on means of identification replacing the personal identifier and the use of identification codes (hereinafter the "data link register") uses an identifier other than natural identification data, the user may prove his identifier and identity using the service *eAzonosítás* (eIdentification) in place of an identifier verification card.

(6) The digital citizen identifier does not exclude the use of any other unique identifier; however, the user shall not be required to use any other unique identifier in the digital space.

(7) In the case of the identification of a digital citizen by means of the service *eAzonosítás* (eIdentification) under this Act, the party requesting identification shall be entitled to access and process the digital citizen identifier following successful identification of the digital citizen.

Section 11 (1) For using the user profile of a natural person, activation shall be required.

(2) Digital citizenship shall be established upon the activation of the user profile at the request of the user. A user profile may be activated, without appearing in person, following successful identification in accordance with section 63 by means of registration in the framework application (for the purposes of this subtitle, hereinafter the "registration"). For a user, who does not yet possess a digital citizen identifier at the time of registration, the organ keeping the register shall generate a digital citizen identifier.

(3) Unless otherwise provided in a government decree, following activation, the user shall be deemed to have provided that he intends to use the service in accordance with this Act for all matters that can be administered in the digital space.

(4) The organ keeping the digital citizenship register shall transfer the following to the organ keeping the client settings register for the purpose of entry into the client settings register:

a) the provision by the user referred to in paragraph (3), upon the activation of the user profile; and

b) the deletion of the provision referred to in point a) and the provision excluding electronic communication, at the same time as the deactivation of the user profile.

Section 12 (1) The purposes of the register shall be the following:

a) providing data as regards the active or inactive status of a user profile, a digital citizen identifier, as well as other data kept in the registers;

b) processing data and technical identifiers required for the identification of a person concerned with a view to ensuring the authenticity of the service and the protection of the rights and legitimate interests of others in connection with an electronic identification service provided as a mandatory government service;

c) supporting services provided by the digital citizenship service provider.

(2) For the purpose of generating a digital citizen identifier, the organ keeping the register shall receive the following from the register of personal data and addresses:

a) natural identification data, citizenship data, sex data and personal identifier of the person referred to in section 10 (1), and

b) number, type, and validity data of the official document verifying identity of the person referred to in point a) that was used for registration.

(3) The organ keeping the register shall receive from the client registration database the data referred to in section 43 (2) of a person, referred to in section 10 (1), who uses an electronic identification service provided as a mandatory government service.

(4) If a user of an electronic identification service provided as a mandatory government service is registered in

a) the register of foreign nationals using electronic administration; or

b) the central aliens policing register, but not in the register referred to in point a);

the organ keeping the register shall receive the data referred to in section 43 (2) from the client registration database.

(5) The organs maintaining the register of personal data and addresses and the register referred to in paragraph (4) b) shall generate an assignment code for the purpose of data transmission to the organ keeping the register. The assignment code shall not contain any person identification data of the data subject and the generation rules shall be designed in a manner that prevents the identification of the data subject.

(6) With regard to the database, the rules on the client registration database and the registration into the database shall apply, subject to the derogations set out in this section. The organ keeping the client registration records shall provide data to the organ keeping the digital citizenship register in accordance with this section.

Section 13 (1) The register shall contain the following data:

a) if the user profile of the user is activated, deactivated or terminated, a reference to this fact and the relevant date, as well as the digital citizen identifier;

b) the data received in accordance with section 12 (2) to (4) other than a reference to the validity of the official document verifying identity, the reason for, and the date of, the natural person user being removed from the register of personal data and addresses, as well as the assignment code referred to in section 12 (5);

c) the electronic mail address and other contact details of the user;

d) data referred to in section 46 (7) relating to an electronic identification service to be provided as a mandatory government service;

e) data required for the identification of the storage related to an electronic registered delivery service;

f) technical data required for the operation of the framework application provided by the digital citizenship service provider to the user, and technical data relating to framework services provided through the framework application.

(2) In respect of the data referred to in paragraph (1) a) and d) to f), the register shall qualify as a publicly certified register.

(3) To ensure that the data processed are up-to-date and that data are verified for the purpose of electronic identification, the organ keeping the register may request data by means of the assignment code referred to in section 12 (5) from the registers referred to in sections 12 (2) and 12 (4) b). From the register referred to in section 12 (2), data as regards a person holding a digital citizen identifier may be requested also by means of the personal identifier. The right to request data shall cover the natural identification data, nationality, and person identifier of the user, as well as, where applicable, a reference to his removal from the register and the date of such removal.

(4) The organ keeping the register may provide data to the organ authorised to process natural identification data and digital citizen identifiers for the purposes of accessing and certifying a digital citizen identifier, and providing information on whether the status of the user profile is active or deactivated.

(5) Without consent from the user concerned, the organ keeping the register may provide the data processed in relation to the user to the following organs:

a) the court, for the purposes of verifying the correctness of a statement of fact made in relation to a person involved in a proceeding pending before the court or the authenticity of data contained in a deed presented, conducting a criminal proceeding, and enforcing a penalty or a measure;

b) an investigating authority, for the purposes of preventing, or detecting a criminal offence, conducting a criminal proceeding, and enforcing a penalty or a measure;

c) the prosecution service, for the purposes of carrying out its tasks, as specified in the Act on the prosecution service, relating to the protection of public order and the supervision of legality, as well as preventing or detecting a criminal offence, conducting a criminal proceeding, and enforcing a penalty or a measure;

d) a national security service, for the purpose of carrying out its tasks;

e) the organ performing internal crime prevention and crime detection tasks that is designated in a government decree, as specified in the Act on the police, for the purpose of performing its internal crime prevention and crime detection tasks;

f) a counter-terrorism organ specified in the Act on the police, for the purposes of preventing, detecting or interrupting a criminal offence, as well as carrying out its counter-intelligence, intelligence, and personal and facility protection tasks.

Section 13/A An organisation keeping a publicly certified register and a digital service provider may process the digital citizen identifier for the purposes of identifying the user and providing services in the digital space.

Section 14 (1) If a natural person user dies, the organ keeping the register of personal data and addresses shall provide data to the organ keeping the register about the reasons for, and date of, the removal of the data subject from the register, for the purpose of deleting the digital citizen identifier.

(2) Upon notification in accordance with paragraph (1), the organ keeping the register shall terminate the user profile of a digital citizen.

(3) The organ keeping the digital citizenship register shall block the data of a natural person upon the expiry of 5 years following the deletion of the digital citizen identifier; thereafter, blocked data shall be processed for 50 years following the deletion of the digital citizen identifier, exclusively for the purposes of tracing the authenticity of a statement relating to digital citizenship and of the electronic identification, as well as the protection of the rights and legitimate interests of citizens.

Section 14/A (1) The organ keeping the register shall record information relating to data processing operations performed within the register in an automated data processing system (hereinafter the "log system") for the purposes of the verification of the lawfulness of data processing operations carried out by electronic means using personal data, and ensuring the integrity and security of personal data.

(2) The log system shall collect the information describing events relating to data processing operations performed within the register and IT applications supporting the services of the register (hereinafter the "log entry").

(3) A log entry shall include the following:

a) the scope of personal data affected by the data processing operation,

b) the legal basis, purpose, and reason for the data processing operation,

c) the exact date and time of carrying out the data processing operation;

d) the name and user identification data of the organisation, person or electronic information system performing the data processing operation, and the data describing its activity;

e) the data relating to the preservation period;

f) other descriptive and technical data relating to the data processing operation.

(4) A log entry shall be generated for all operations performed with personal data, upon the occurrence of the data processing event. A log entry shall be provided with accurate and unalterable time data.

(5) Data recorded in the log system shall be accessed and used only for verifying the lawfulness of data processing, enforcing data security requirements, and conducting a criminal proceeding, as well as for the purposes of detection, national security protection and counter-intelligence, intelligence and national security and crime prevention control.

(6) The organ keeping the register shall transfer data from the log system to the National Authority for Data Protection and Freedom of Information and, upon request, to a person or organisation carrying out an activity specified by law for a purpose referred to in paragraph (5). The organ keeping the register shall also log any data provision from the log system.

(7) The log system shall be protected from unauthorised access.

(8) Information relating to operational events of the registration system and the applications supporting the services of the register, concerning application operation as well as network and system operation, shall not be collected in the log system.

(9) The preservation period of a log entry in the log system shall be ten years from generation. Upon the expiry of the preservation period, the log entry shall be deleted without delay, except where the log entry is required for a verification proceeding already launched. In such an event, deletion shall be performed upon the conclusion of the proceeding.

Section 14/B (1) For the purposes of protecting data processed by the organ keeping the register in the register against access or alteration without authorisation, disclosure, deletion, damage or destruction, as well as the verification of the lawfulness of data processing, the organ keeping the register shall keep an authorisation register of organs subject to an obligation to provide data for the register by electronic means using a specific IT application, organs processing data in the register, organs authorised to receive or request data directly, and users holding access authorisation on behalf of organs authorised to receive or request data directly.

(2) The register referred to in paragraph (1) shall contain, as regards an organ referred to therein, the following:

a) name;

b) seat and postal address;

c) electronic mail address and phone number;

d) for a person holding access authorisation on behalf of the organ:

da) family and given name;

db) family and given name at birth;

dc) mother's name;

dd) place and date of birth;

de) organisational unit;

df) type, scope and legal basis of access authorisation;

dg) reference to the fact that the access authorisation was granted or cancelled, and the relevant date;

dh) user name;

di) electronic mailing address used for official communication.

(3) A person required to provide data, processing data in the register, or authorised to directly receive or request data from the register shall have access authorisation for a definite period of two years. At the expiry of the definite period, the access authorisation shall be renewed upon application by the organ requesting the authorisation.

(4) Personal data processed in the register referred to in paragraph (1) shall be retained for ten years from the cancellation of the last authorisation of the user.

(5) An organ with direct access authorisation shall request the entry of its users into the register referred to in paragraph (1) by submitting an application for direct access authorisation to the organ keeping the register. An application for direct access authorisation shall contain the data referred to in paragraph (2) a) to c) and d) da to df) and di) as well as the personal identifier of the person holding access authorisation on behalf of the organ. On the basis of the application, the organ keeping the register shall process the personal identifier provided in the application for the purpose of making use of data provision to verify identity in the register of personal data and addresses, for as long as necessary to this end. Organs with direct access authorisation shall notify the organ keeping the register of any change in the data listed in paragraph (2) by electronic means, within three working days of the change.

(6) To verify the lawfulness of data processing, the Minister responsible for professional supervision, the National Authority for Data Protection and Freedom of Information and the organ requesting access authorisation may request all data processed in the register referred to in paragraph (1) from the organ keeping the register.

7. General rules of data processing

Section 15 (1) When using a service in the digital space and in the course of administration of matters in accordance with this Act, the digital citizenship service provider and the supporting service provider shall access and process all personal data of the user that are necessary for the provision of the digital service used, for the purpose of ensuring the efficiency and high quality of digital services, reducing administrative time limits and other administrative burdens relating to the matter, and establishing an integrated procedure affecting multiple sectors simultaneously.

(2) In the context of the data processing referred to in paragraph (1), the digital citizenship service provider shall be entitled, as digital data controller, to receive and transfer, in addition to data referred to in paragraph (1), the types of data referred to in paragraph (3) to the extent necessary and sufficient for the provision of the service.

(3) All personal and other data necessary for the successful provision of the service that are processed by an organisation performing a public duty shall constitute data that may be processed pursuant to paragraph (2).

(4) Further detailed rules of data processing in connection with data processing pursuant to paragraphs (2) and (3) shall be laid down in a government decree issued on the basis of authorisation by this Act.

(5) The digital citizenship service provider may request data in accordance with the government decree referred to in paragraph (4) from the organisation recording the data; the entity shall comply with such a request.

Section 15/A The provider, specified by law, of a life-event-based service and a service relating to European Digital Identity Wallet, as well as an organ involved in the provision of the services shall access and process all personal data of the user that are required for the provision of the service under this section.

Section 16 (1) For the purpose of ensuring seamless access without unnecessary administrative burdens to services that are available in the digital space pursuant to this Act, state registers and specialised systems and databases not qualifying as a state register may be linked for the period of, and to the extent necessary for, administering specific matters and using services.

(2) Linking shall be permissible only in connection with a digital service requested by the user.

Section 17 (1) Proactive services specified in a decree of the Government may be provided without a specific application or a request for using the service.

(2) A proactive service shall primarily serve to provide information relating to a life-event based and other digital services that facilitate compliance with obligations and the exercise of rights.

(3) For the purpose of providing proactive services, the personal data of users may be processed. The user may make a statement that he does not consent to the processing of his personal data in the context of a proactive service.

PART THREE

ELECTRONIC ADMINISTRATION

Chapter II

BASIC RULES OF ELECTRONIC ADMINISTRATION

8. General rules

Section 18 (1) Unless otherwise provided by an Act or a government decree, a user shall take his administrative acts by electronic means in accordance with this Act, and make his statements by electronic means, before the digital service provider in the course of the administration of matters in the digital space.

(2) Electronic administration shall not be applied in the following cases:

a) for procedural acts, where the Act or government decree expressly requires the user to appear in person;

b) for a procedural act, in respect of which it cannot be construed;

c) for proceedings and procedural acts, where it is prohibited by an international treaty or a directly and generally applicable mandatory legal act of the European Union; as well as

d) for a record, deed or other submission that contains classified data.

(3) An Act or a government decree may restrict the possibility of using electronic administration only if, in the course of the proceeding, the appearance of the user in person, or the submission of a deed the submission of which cannot be substituted for by any other means, is indispensable.

(4) A digital service provider shall operate, either independently or in cooperation with other digital service providers, a customer service that may be contacted by phone or by other electronic means, in accordance with the rules on undertakings providing public services of the Act on consumer protection, with the derogation that the customer service shall be available at least 40 hours per week. Based on a separate agreement, the organs referred to in section 9 (2) a) to i) may ensure that the tasks set out in this paragraph are carried out by means of a national call centre designated in a decree of the Government.

(5) For a service provided under this Act, a restriction on the age of the user may be introduced as a condition for using the service. Compliance with the age requirement shall be verified by means of either the relevant function of the service in question or the register required for the provision of the service.

9. Mandatory electronic administration

Section 19 (1) Unless otherwise provided by an Act, on the basis of an obligation arising from an international treaty, an international treaty, or a directly applicable legal act of the European Union, the following shall administer matters electronically:

a) if acting as a user in the context of a digital service provided by an organ required to provide a digital service,

aa) an economic operator;

ab) an organisation listed in section 3 of Act CXCV of 2011 on public finances;

ac) a prosecutor;

ad) a notary;

ae) another administrative authority not falling within the scope of subpoints ab) to ad); and

b) the legal representative of a user in the context of a digital service provided by an organ required to provide a digital service.

(2) Section 27 shall apply accordingly to the service of a document sent to a user or legal representative referred to in paragraph (1), a user required by an Act to administer matters electronically, as well as a holder of an active user profile.

(3) In addition to the situations listed in paragraph (1), a user and its legal representative shall be required to administer matters electronically only in the cases specified by an Act and only if electronic administration can be construed in relation to the given administrative act.

(4) With the exception set out in the Act on the more efficient operation of companies under public ownership, only an Act may impose an obligation on a natural person to administer matters electronically.

(5) With the exception of cases specified in an Act or government decree, if electronic communication or a method of electronic communication is required by law for making a statement, any statement that does not comply with this requirement shall be invalid.

10. Method of electronic administration

Section 20 A user shall make any statement, perform any procedural act, or fulfil any other obligation required for electronic administration

a) primarily by means of the digital citizenship framework application;

b) by means of the single customised administration platform; or

c) by electronic means in accordance with the information published by the digital service provider.

11. Automated decision-making procedure

Section 21 (1) An organ required to provide a digital service shall conduct the proceeding using automated decision-making if

a) for a case commenced upon application, the user submits his application by electronic means;

b) decision-making does not require deliberation; or

c) the data required for administering the matter are available to the digital service provider in a form suitable for automated processing, or the digital service provider receives such data by means of automated information transfer in a format suitable for automated processing.

(2) If automated decision-making applies, the organ required to provide a digital service shall make its decisions concluding the proceeding, or decisions otherwise required for administering the matter, without human involvement, and ensure that they are communicated to the user. Where the decision was made in an automated decision-making proceeding, the organ required to provide a digital service shall inform the user accordingly.

(3) Any other decision or notification required for administering a matter may be made without human involvement, even if the proceeding is conducted by the organ required to provide a digital service by means other than automated decision-making.

(4) Automated decision-making procedure shall not be permissible if it is prohibited by an Act or government decree in relation to the matter concerned.

12. Records and documents

Section 22 (1) In the digital space, documents shall be generated in an electronic form. A record may be issued in a paper-based format only in exceptional cases.

(2) In the course of electronic administration, a digital service provider shall, as necessary,

a) produce, or have produced, an authentic electronic copy of a record received in a paper-based format;

b) produce an authentic paper-based copy of a decision issued by electronic means, or have it converted into an authentic paper-based record.

(3) An electronic document shall have the same probative value as the original paper-based document, where

a) an authentic copy is produced pursuant to the rules of producing electronic copies of paper-based documents;

b) an authentic copy is produced pursuant to the rules of converting electronic records into authentic paper-based records.

(4) A document shall have the same probative value as the original electronic document, provided that it was produced in line with the rules on converting electronic documents into authentic paper-based documents or on the central electronic administration service for producing electronic copies of electronic documents in other formats.

13. Electronic administration through an electronic point of contact

Section 23 (1) The provisions of this Act shall apply to using an electronic point of contact referred to in section 34 (6) of Act LXVI of 1992 on the registration of personal data and address of citizens (hereinafter the "Registration Act") (hereinafter "electronic point of contact") with the derogations provided for in this section.

(2) An application submitted through an electronic point of contact following electronic identification shall be regarded as submitted electronically by the user in accordance with the provisions of this Act.

(3) If the technological conditions are met, a matter may be administered through an electronic point of contact even if, by law or by the nature of the matter, it is to be administered solely in person. In such a situation, it shall be regarded as if the user had acted in person.

(4) If an electronic point of contact is used, the service referred to in section 12/B of Act CLXXXVIII of 2015 on the facial image analysis register and the facial image analysis system (hereinafter the "Facial Image Analysis Act") may also be used for verifying the identity of a user. In such a situation, a person may take the juridical act requiring identification only if he is registered in the register of personal data and addresses. Identification through this service shall be considered equivalent to electronic identification under this Act.

(5) A biometric identifier (facial image, fingerprint, and signature) recorded via an electronic point of contact shall be regarded as equivalent to a biometric identifier recorded by an authority authorised to record facial images and signatures in a standardised manner.

Chapter III

ELECTRONIC COMMUNICATION

14. Basic rules

Section 24 (1) Communication shall be deemed electronic if a user makes its statement, or a digital service provider makes its statement or its decision (hereinafter jointly "statement"), by electronic means. The law may permit the user to perform a procedural act requiring appearance in person by means of electronic communication.

(2) Electronic communication shall also include voice communication, as well as electronic communication ensuring the transfer or recording of an audio-visual recording, unless that is impossible by definition.

15. Means of contact

Section 25 (1) Upon the activation of a user profile, the organ keeping the digital citizenship register shall transfer the data referred to in section 13 (1) e) that are required for the identification of the storage for the user profile of the natural person to the organ keeping the register of administrative settings, which shall record such storage as the official means of contact of the natural person user in the register of administrative settings (hereinafter the "client settings register").

(2) The official means of contact of a natural person user shall be the official means of contact he reported to the client settings register, or the storage referred to in paragraph (1).

Section 26 (1) If a user is an economic operator, it shall report its electronic contact address as official means of contact (hereinafter "official contact address") to the client settings register within eight days following registration, unless an Act provides otherwise, or within 8 days following establishment, where the registration in a register introduced by law is not mandatory for the operation of the economic operator; such an official contact address may be

a) either an electronic registered delivery service address; or

b) an *ePosta* (ePost) address.

(2) Economic operators shall report to the client setting register any change to their official contact address referred to in paragraph (1), specifying the date of the change.

(3) The Government shall designate in a decree the service provider that provides to the organs specified in a decree of the Government with a contact address referred to in paragraph (1) under a separate public service contract free of charge.

(4) If an economic operator user does not possess an official contact address referred to in paragraph (1), the digital service provider may conduct the proceeding also without electronic communication, with the proviso that the digital service provider shall initiate a supervision of legality proceeding or an administrative audit, as defined by an Act, against the economic operator for failing to meet its obligation.

(5) If an economic operator is recorded in a publicly certified register, the organ keeping the register shall transfer, by electronic means and without consideration, all recorded public information concerning the economic operator that are required for the identification of the economic operator and its authorised representative, to the organ keeping the client settings register or the service provider of the electronic registered delivery service address, as specified by the economic operator, with a view to registering and operating the official contact address. The organs concerned shall lay down the technical rules of completing such data provision in an agreement.

(6) Private entrepreneurs shall report their official contact address as required by a decree of the Government.

(7) The organ keeping the register shall transmit, data recorded in the client settings register to the Hungarian Central Statistical Office (hereinafter the "HCSO") free of charge for the purpose of defining the group of data providers; HCSO shall be authorised to process such data for statistical purposes. As regards a natural person user, the organ designated by the Government shall provide data also by way of direct query. HCSO shall process the data received or retrieved in a process for statistical data generation. Upon the termination of a task, and in particular upon closure of individual data recording activities, HCSO shall delete data received in connection therewith.

(8) The organ keeping the register shall transmit all data recorded in a register referred to in paragraph (1) relating to an economic operator to HCSO free of charge for the purpose of defining the group of data providers; HCSO shall be authorised to process such data for statistical purposes.

Section 27 An item served at an official contact address referred to in sections 25 and 26 shall be considered served

a) at the time specified in the confirmation of receipt if the service provider providing the official contact address confirms receipt by the user;

b)

c) on the fifth working day following the date of the second notice if the service provider providing official contact address confirms that the addressee did not receive the item despite having been notified twice.

Section 28 If a user indicates, in a statement addressed to the digital service provider, his electronic mail address, his phone number suitable for receiving short text messages or any other means of contact suitable for electronic communication, the digital service provider may use the provided contact address to communicate with the user for information purposes. Where the user also has an official contact address, the digital service provider shall communicate with the user through the official contact address; the means of contact under this section shall be used exclusively for notification and information.

Section 28/A Where a natural person user does not possess an official contact address within the meaning of section 25 (2), the organ required to provide a digital service may attempt to serve the item at the storage, referred to in section 46 (5), if known to it. In such a situation, section 27 shall apply with the proviso that after the second failed service attempt, the organ required to provide a digital service shall make other arrangements for the service of the record or the notification.

16. Method of communication

Section 29 (1) A user shall select the method of electronic communication with the digital service provider on the basis of the means of contact specified in the information published by the digital service provider.

(2) When making statements addressed to the user, the digital service provider shall communicate with the user through his official contact address, unless the law specifies other method of communication.

Section 30 (1) Where a written statement is required by law for the purpose of non-electronic administration, a juridical act made through electronic communication shall qualify as such a statement, provided that

a) the person making the statement is identified by electronic means pursuant to section 34 (2); and

b) it is guaranteed that the electronic document served corresponds to the document approved by the person making the statement.

(2) With regard to statements other than those mentioned in paragraph (1), an Act or a government decree may provide that such a statement shall have the legal effect of a written statement.

(3) Unless excluded by law, a statement made by electronic means ensuring voice transmission by an identified user shall have the same legal effects as an oral statement made by non-electronic means.

17. Administration using communication via video technology

Section 31 (1) In compliance with the detailed rules laid down in this subtitle, a digital service provider may communicate with the user by means of a system suitable for transferring an audio-visual recording based on a live video telecommunication channel provided by the organ designated in a decree of the Government. For the purposes of this section, the organ designated in the decree of the Government shall be considered an organ providing an electronic identification service.

2) When using the system referred to in paragraph (1), a user shall identify himself using his natural identification data that is available at the digital service provider or provided by the user,

a) by verifying his facial image produced using the service referred to in paragraph (1) in accordance with the detailed rules laid down in paragraph (3) and a decree of the Government, provided that his data are recorded in the register of personal data and addresses; or

b) by the identification means referred to in Article 6 (1) of the eIDAS Regulation, provided that his data are not recorded in the register of personal data and addresses.

(3) In the course of the identification referred to in paragraph (2) a), the system referred to in paragraph (1) shall compare the natural identification data, nationality and verification card number, that is read from an official verification card suitable for verifying identity (for the purposes of this subtitle, hereinafter the "official document") with the natural identification data recorded in the register of personal data and addresses, verify the validity of the official document, and verify, using automated comparison as defined in Subtitle 9/B of the Facial Image Analysis Act, whether a facial image of the user, produced by means of video signals, matches the facial image that was recorded in the register of personal data and addresses when the person subject to verification was entered into the register the last time. Identification shall be considered successful if the data recorded in the register match, the official document is valid, and the required threshold of match is reached.

(4) For the purposes of ensuring the possibility of *ex post* enforcement of rights, protecting the procedural rights of the user, and verifying *ex post* whether certain administration-related rights and obligations are respected; in the course of identification under paragraph 2 a) and administration under paragraph (1), subject to the exception provided for in paragraph (5), the organ designated in a decree of the Government shall, on behalf of the digital service provider, record, and retain for 1 year after recording, in a traceable manner, as an audio-visual recording, in a manner that excludes the deterioration of the quality of the recording, the full communication between the digital service provider and the user, as well as the detailed information provision as regards the identification of the user by means of video technology and the related consent by the user.

(5) A digital service provider shall not retain a recording made in the course of administration under paragraph (1) if

a) the user did not make a substantial statement in the matter or he makes such a statement as a private deed of full probative value within the meaning of the Act on the Code of Civil Procedure; and

b) a facial image or signature is not recorded in accordance with paragraph (7).

(6) In a situation, and for a reason, referred to in paragraph (4), a digital service provider shall be entitled to record and store an image of the official document for the period specified in paragraph (4).

(7) Where, in a matter administered using the means of communication referred to in paragraph (1), an Act requires the recording of the facial image and the signature of the user, the digital service provider may record

a) the facial image;

b) the signature, in cases specified by law;

also using the system referred to in paragraph (1).

(8) The organ designated in a decree of the Government shall process, until verification is successful, the data referred to in paragraph (2) of the user, and shall be entitled to receive such data from the register of personal data and addresses, through the link register if required.

Section 32 (1) Where the signature of the user or the representative of the digital service provider is required by law for the validity of the statement of the user, such a signature may be substituted in accordance with a decree of the Government when using the system referred to in section 31 (1).

(2) Unless an Act or a government decree provides otherwise, a digital service provider shall not communicate any decision requiring a statement of reasons to the user in the course of communication in accordance with section 31 (1).

(3) A digital service provider shall send to the user in writing also a decision that does not require a statement of reasons, provided that the decision was communicated in the course of communication in accordance with section 31 (1). Unless an Act or a government decree provides otherwise, the decision shall be deemed communicated upon service of the written decision.

Section 33 The provision of this subtitle shall not apply to a criminal proceeding, a proceeding under the Act on the enforcement of penalties, measures, certain coercive measures and infraction confinement, a proceeding under the Act on mediation in criminal cases, an infraction proceeding, a contentious proceeding under the Act on the Code of Civil Procedure, as well as a non-contentious court or notarial proceeding.

Chapter IV

RIGHTS AND OBLIGATIONS OF THE USER

18. Electronic identification obligation

Section 34 (1) With the exception set out in section 30 (2) and unless the law provides otherwise, the user shall be entitled to electronic administration without electronic identification if the performance of the given procedural or administrative act or the making of the given statement does not require the provision of person identification data if carried out through non-electronic administration.

(2) In a situation not covered by paragraph (1), a user using electronic administration may identify himself using, at his own discretion,

a) an electronic identification service, including identification with a digital citizen identifier; or

b) an electronic identification means meeting the requirements specified in Article 6 (1) of the eIDAS Regulation

that ensures that the name of the user is available to the digital service provider, and his further data required for identification are available to the electronic identification service provider.

(3) Subject to the consent of the user, the organs listed in section 9 (2) a) to i) may request the organ keeping the client registration records referred to in section 43 (1) of the electronic identification service, or another organ storing the data of the user relating to an electronic identification means or solution referred to in paragraph (2), to provide identification data required for administering the matter that may be processed by the digital service provider.

(4) The digital service provider shall be entitled to request and process data in accordance with paragraph (3) from the time when the digital service provider becomes aware of the intention of the user to administer a matter.

(5) Unless the law provides otherwise, a digital service provider shall itself determine the assurance level of the electronic identification under Article 8 (2) of the eIDAS Regulation it requires in the course of electronic communication requiring electronic identification of the user. Unless the law or the digital service provider provides otherwise, assurance level low, as specified in Article 8 (2) a) of the eIDAS Regulation shall be sufficient for electronic identification.

Section 35 (1) An economic operator user may, by electronic means, perform a procedural act or make a juridical act requiring electronic identification following

a) its electronic identification pursuant to section 34 (2); or

b) the electronic identification of its representative, who is a natural person user, pursuant to section 42 and the verification of the right of representation.

(2) On behalf of the represented person, the representative of a natural person user may perform or make, by electronic means, a procedural act or juridical act requiring electronic identification following his electronic identification pursuant to section 34 and the verification of his right of representation.

(3) A digital service provider shall not require the user or its representative to provide proof of the right of representation of the representative if

a) the data proving the right of representation is required to be kept in a register established by the law as publicly certified data,

b) the user granted authorisation, under his administrative settings, to the representative to perform a procedural act or make a juridical act.

(4) If paragraph (1) b) applies, the electronic identification service provider shall transmit to the digital service provider the natural identification data of the natural person acting on behalf of an economic operator user, for the purpose of identifying the representative. The digital service provider shall be responsible for the lawfulness of data processing.

(5) The submission of an electronic statement through a machine interface used by the economic operator user regarding a matter where the identification of its representative is either unnecessary or guaranteed by other means, in particular on the basis of natural identification data provided by the economic operator user or a trust service certificate used by the representative, shall be considered equivalent to the identification of that representative pursuant to paragraph (1) b).

(6) Electronic communication with the economic operator user through a machine interface operated by the organ required to provide a digital service shall be considered equivalent to the identification of the economic operator pursuant to paragraph (1) a), provided that the identification of the economic operator user is ensured on the basis of prior registration for this purpose. Registration through the electronic administration platform established for this purpose by an organ required to provide a digital service shall be carried out following the electronic identification of the statutory representative, who is a natural person, of the economic operator user pursuant to section 34 (2) and the verification of the right of representation. When using the machine interface service, the user shall be presumed to be an economic operator previously registered for the purpose of using the service.

19. Obligation to certify identifiers and data

Section 36 (1) A digital service provider listed in section 9 (2) a) to i) shall not request the user to attest any data, other than data required for the identification of the user, that was published by the organ concerned in compliance with an obligation under the Act on the right to informational self-determination and on the freedom of information, or that is to be included in a publicly certified register introduced by law.

(2) Where the digital service provider obtains the data referred to in paragraph (1) by means of information transmission, the period of up to 3 working days that is required for fulfilling the request shall not be calculated into the administrative time limit, except for authority proceedings falling within the scope of the Act on the Code of General Administrative Procedure.

Section 37 (1) Where the user is required by law to attest an identification code, introduced by an official verification card, for which an encrypted assignment code is recorded in the data link register, the user may comply with this request in the course of electronic or non-electronic administration before the digital service provider also by presenting another official verification card suitable for verifying identity that attest any other such identification code.

(2) Where the service is used through a user profile, the user shall not be required to provide an identification code other than the digital citizen identifier.

(3) Where the law requires the user to provide an identification code, introduced by an official verification card, that is recorded in the data link register, the user may comply with this request in the course of electronic or non-electronic administration before the digital service provider also by attesting the identification code introduced by an official verification card of a register connected to the data link register.

(4) If paragraphs (1) to (3) apply, the digital service provider shall obtain, through the data link register, the identifier it is authorised by law to process.

(5) If a data controller that is connected to the data link register uses, on the basis of authorisation by an Act, an identifier other than natural identification data, its user may also attest the identifier and his identity using an identification service in place of a verification card certifying the identifier used by the data controller.

(6) After the requested identification code is provided, the proceeding organ, unless it is authorised by an Act to process such data, and the operator of the link register shall delete without delay all identification data provided by the user for the purpose of service provision.

20. The right of the user to settings

Section 38 (1) A user may make juridical acts, as part of its administrative settings, before an organ designated in a decree of the Government with respect to the following matters:

a) juridical acts concerning representation;

b) using the automated data change reporting service referred to in section 15 (3) of Act XXII of 2022 on certain matters relating to the operation of territorial public administration and amending certain Acts in connection with the Fourteenth Amendment to the Fundamental Law.

(2) The activation of a user profile for digital citizenship by the user, as referred to in section 11 (2), shall be deemed to constitute a setting by the user enabling electronic communication.

(3) As part of the administrative settings, the user may

a) request a service provider specified in a decree of the Government to notify by electronic means, automatically or based on an *ad hoc* instruction by the user, a digital service provider specified as part of the administrative settings about changes to any data of the user specified by him;

b) may grant authorisation, addressed to one or more than one digital service provider or all digital service providers, to another legal entity specified by law to represent him before a digital service provider in specific, or all, matters;

c) make instructions as to which of his administrative settings may be accessed by which digital service provider, provided that he also indicates, within this scope, which administrative settings are effective *vis-á-vis* which digital service provider; and

d) make any other juridical act specified by law.

(4) Unless provided otherwise by law, administrative settings may be applied or modified

a) in person; or

b) by electronic means using the platform provided by the service provider designated by the Government.

(5) If the law requires a juridical act to be made in writing or embodied in a private deed of full probative value, a statement made as part of the administrative settings shall be deemed to satisfy that requirement.

(6) A setting concerning a matter shall be invalid, if it is inconsistent with the laws applicable to the given matter.

(7) In a pending matter launched through an identification service referred to in section 46 (1) b), after the launch of the matter, the digital service provider shall observe any new or modified administrative setting recorded in the client settings register only if the user reports it to the digital service provider as well.

(8) An Act or a government decree may provide that a juridical act referred to in paragraph (1) a) shall only be valid if the authorisation is accepted and the acceptance is recorded in the client settings register.

(9) Except where the user is a natural person or a private entrepreneur, the setting referred to in paragraph (1) a) shall not be applied as regards matters falling within the competence of the state tax and customs authority, other than matters falling within the functions of the state tax and customs authority as an investigating authority.

Chapter V

OBLIGATIONS OF THE DIGITAL SERVICE PROVIDER

21. Digital service provision

Section 39 (1) A digital service provider shall ensure the rights of the user as provided for in this Act by means of an information system providing a digital service in accordance with this Act and its implementing decrees.

(2) In the information system referred to in paragraph (1), the digital service provider shall ensure at least the following:

a) possibility of using the digital service by means of the framework application;

b) possibility of using digital framework services;

c) query of the administrative settings of the clients;

d) possibility of administering matters through a custom front office;

e) where a service requiring electronic identification is provided, the use of electronic identification solutions accessible through the central identification agent service by the user;

f) service by means of the electronic registered delivery service as specified in a decree of the Government and the receipt of messages addressed to the user;

g) immediate certification of the receipt of juridical acts made, and records sent, by the user by electronic means, in accordance with the law;

h) processing of electronic documents bearing at least advanced electronic signatures and electronic seals that meet public administration requirements;

i) production of documents authenticated in accordance with this Act;

j) service of records on the user by means of any type of service referred to in section 26;

k) in the case of an organ listed in section 9 (2) a) to i), payment, by electronic means, of burdens relating to a proceeding; and

l) processing of electronic forms generated by means of an electronic form filling service.

(3) Organs listed in section 9 (2) a), b), d) to f) and section 80 (1) a) to h) shall ensure the continuous availability of the information system referred to in paragraph (1).

(4) Where the entire administrative process can be carried out through electronic administration solutions, a digital service provider shall ensure, by means of electronic administration solutions supporting the entire administration process, electronic administration for the user, unless prohibited by an Act or the administrative settings of the client.

(5) A law

a) may designate a digital service provider, from among organs with identical competences, that is granted exclusive authorisation to administer the given matter by electronic means in the entire country;

b) may provide that, when using electronic administration, each organ of identical subject-matter competence may proceed with territorial competence over the entire country, and that the matters shall be distributed automatically on the basis of objective criteria.

(6) The State shall provide, free of charge, the organs listed in section 9 (2) with the framework services and supporting services that are required for the operation of the information system ensuring the digital service referred to in paragraph (2).

(7) The digital service providers specified in a decree of the Government shall, unless a more stringent requirement is set by the law, back up administration-related information systems, registers and data, as specified in a decree of the Government, at a frequency and in accordance with the procedure specified in a decree of the Government, and shall send such security backups to the organ designated by the Government as responsible for data retention. The organ responsible for data retention shall not consult the content of data backups.

Chapter VI

REGULATED ELECTRONIC ADMINISTRATION SERVICES

22. General rules of regulated electronic administration services

Section 40 (1) Regulated electronic administration services shall be the following:

a) electronic identification services;

b) electronic registered delivery services;

c) services relating to electronic signatures that may be used for the provision electronic administration services and meet the requirements laid down by law;

d) services classified as regulated electronic administration services in a government decree issued on the basis of authorisation by this Act.

(2) More than one regulated electronic administration service may be implemented and provided as a bundle; in such a scenario, the service provider shall meet all requirements concerning each regulated electronic administration service separately.

(3) The provisions laid down in the Act on the general rules on taking up and pursuing service activities shall apply to supporting service provision, with the derogations provided for under this subtitle and in a decree of the Government, accordingly.

(4) The use of a regulated electronic administration service may be made mandatory by an Act or a government decree.

(5) The provision of regulated electronic administration services shall be conditional upon ensuring compliance with the cybersecurity requirements laid down in a decree by the president of SARA.

23. Electronic identification services

Section 41 (1) An electronic identification service may be used by a person who, in order to use the service, registers and is recorded in the client registration records, as specified in section 43 (1), of the electronic identification service provider.

(2) A user may register to use an electronic identification service

a) by electronic means using an electronic signature, an electronic identification means meeting the requirements laid down in Article 6 (1) of the eIDAS Regulation, or another identification service, the registration for which meets the requirements laid down in this subtitle; or

b) in person, through a proceeding that meets the requirements laid down in this subtitle.

Section 42 (1) Before registration, a natural person user (for the purposes of this subtitle, hereinafter the "applicant") shall appear in person before the electronic identification service provider or the registration organisation acting on behalf of the electronic identification service provider (hereinafter jointly the "client registration organ"). In a situation determined by the electronic identification service provider, a proceeding conducted by the registration organisation at an external site shall be deemed equivalent to the user appearing in person, provided that the identity of the applicant can be verified, under security conditions that are at least equivalent, as required by this subtitle.

(2) A natural person who appears in person shall be identified by the client registration organ on the basis of data indicated on an official verification card suitable for verifying identity that is presented by the natural person. The client registration organ shall compare the natural identification data of the natural person, as indicated on his official verification card, to data recorded in

a) the register of personal data and addresses;

b) the central aliens policing register, if the natural person is a foreign national who is not recorded in the registers referred to in points a) and c);

c) the register of foreign nationals using electronic administration.

(3) If an applicant is recorded in the register referred to in paragraph (2) a), the client registration organ shall transfer the birth name indicated on the official verification card suitable for verifying identity presented, as well as the identifier and type of the official verification card, to the central register of such official documents for the purpose of determining whether the official verification card is authentic and valid, and the facial image and signature data are identical.

(4) The register referred to in paragraph (3) shall transfer to the client registration organ the natural identification data, as well as the data on nationality, the number and validity of the official document, and, if requested by the client registration organ, the facial image and the signature. If the electronic identification service is provided as a mandatory government service, the transfer of facial image and signature data shall be mandatory.

(5) If the applicant is recorded in the register referred to in paragraph (2) b), the central aliens policing register shall transfer to the client registration organ, upon data request, the natural identification data, as well as data on nationality and, if requested by the client registration organ, the facial image and signature. If the electronic identification service is provided as a mandatory government service, the transfer of facial image and signature data shall be mandatory.

(6) If the applicant is recorded in the register referred to in paragraph (2) c), the register of foreign nationals using electronic administration shall transfer to the client registration organ, upon data request, the natural identification data, as well as data on nationality, the number, type, and validity of the official document used for registration in the register of foreign nationals using electronic administration, and, if requested by the client registration organ, the facial image and signature. If the electronic identification service is provided as a mandatory government service, the transfer of facial image and signature data shall be mandatory.

(7) The client registration organ shall compare the data received with the data indicated on the document presented, and shall determine whether the facial image corresponds the person appearing before it.

(8) If the data and the facial image are confirmed as a match during a proceeding under paragraph (7), the client registration organ shall receive the data listed in section 43 (2) from the register referred to in paragraph (2), for the purpose of entry into the client registration records.

(9) If the data and the facial image are not confirmed as a match during a proceeding under paragraph (7), or the official verification card presented as proof of identity is invalid, the client registration organ shall refuse to register the client, and shall delete all data already recorded, if any.

(10) All facial image and signature data referred to in paragraphs (4) to (6) shall be deleted without delay after the verification of identity. The client registration organ may use data not recorded in the client registration records only for the purposes of identification and determining whether or not the data match.

(11) An electronic identification service provided for under this Act may only be used by persons recorded in any of the registers listed in paragraph (2).

(12) A person recorded in any of the registers listed in paragraphs (2) b) and c) may use an electronic identification service only in matters falling within the scope of this Act.

Section 43 (1) With a view to ensuring authentic electronic identification and traceability, electronic identification service providers shall keep a register of applicants (hereinafter the "client registration records").

(2) The client registration records shall include the following:

a) natural identification data, nationality, and unique identification number of the applicant; and

b) for an applicant included in the register specified in section 42 (2) c), the data on the number, type, and validity of the official document used for registration in the register of foreign nationals using electronic administration, in addition to the data listed in point a).

The client registration records may include data specified in the standard contract terms of the electronic identification service provider.

(3) As part of its registration procedure, a client registration organ shall issue a certificate concerning the registered data and, where applicable, the identifier generated by it. The applicant shall confirm that the data provided by the applicant as indicated in the certificate are correct by signing in his own hand a printout of the certificate or, where the certificate is generated by electronic means, by means of the electronic identification function of his identification card fitted with a storage component, using an at least advanced electronic signature or the service *eAláírás* (eSignature).

(4) An organ keeping client registration records shall be entitled to request data from any register listed in section 42 (2) for the purposes of verifying data as required for electronic identification and ensuring that the data processed are kept up-to-date. Regarding a person registered in the client registration records, the entitlement to request data shall extend to the following data:

a) natural identification data, nationality, and fact of death of the applicant;

b) for an applicant included in a register specified in section 42 (2) c), the number, type, and data on the validity of the official document used for registration in the register of foreign nationals using electronic administration, in addition to the data listed in point a).

(5) Registration shall be cancelled by an organ keeping client registration records upon

a) request by the user;

b) death of the user;

c) for a person included in the register specified in section 42 (2) c), expiry of the official document used for registration in the register of foreign nationals using electronic administration.

(6) Registration shall also be cancelled if a registration organ is informed that the applicant is not included in any register listed in section 42 (2).

(7) A client registration organ may disclose user data without the consent of the user to the following organs:

a) the court, for the purposes of verifying the correctness of a statement of fact made in relation to a person involved in a proceeding pending before the court or the authenticity of data contained in a deed presented, conducting a criminal proceeding, and enforcing a penalty or a measure;

b) an investigating authority, for the purposes of preventing or detecting a criminal offence, conducting a criminal proceeding, and enforcing a penalty or a measure;

c) the prosecution service, for the purposes of carrying out its tasks, as specified in the Act on the prosecution service, relating to the protection of public order and the supervision of legality, as well as preventing or detecting a criminal offence, conducting a criminal proceeding, and enforcing a penalty or a measure;

d) a national security service, for the purpose of carrying out its tasks;

e) a counter-terrorism organ specified in the Act on the police, for the purposes of preventing, detecting or interrupting a criminal offence falling within its competence, as well as carrying out its counter-intelligence, intelligence, and personal and facility protection tasks.

(8) Data relating to a natural person shall be blocked by a client registration organ upon the expiry of 5 years after the cancellation of registration; subsequently, blocked data may be processed only for the purposes of tracing the authenticity of electronic identification and protecting the rights and legitimate interests of citizens, for a period specified in the standard contract terms of the client registration organ, but not less than 10 years and not more than 50 years following the cancellation of registration.

(9) After data is blocked pursuant to paragraph (8), the client registration organ shall unblock and provide data to an organ listed in paragraph (7) for a purpose specified in paragraph (7).

Section 44 (1) With the exception of a situation described in section 34 (3), an electronic identification service provider, following successful electronic identification in the course of electronic administration, may transfer to the digital service provider the name of the identified person, as well as his electronic mail address, if available, and the assignment code generated for the organ that cannot be deducted from natural identification data.

(2) In the course of performing a request under paragraph (1), an electronic identification service provider shall transfer, upon request by the requesting party, to the regulated electronic administration service provider the personal data processed by the electronic identification service provider as necessary for registration.

24. Regulated electronic administration services provided as mandatory government services

Section 45 (1) The Government shall provide the following regulated electronic administration services acting through a designated regulated electronic administration service provider:

a) electronic identification service referred to in section 46 (1) b) for natural person users;

b) electronic registered delivery service;

c) government authentication service, including the following services:

ca) services relating to electronic signatures and electronic seals that meet the requirements laid down by the law and may be used for providing electronic administration services, and generation of certificates relating to such services for use by digital service providers, as well as regulated electronic administration service providers, and central electronic administration service providers, as defined by this Act;

cb) services relating to electronic time stamps, and generation of identification certificates for use by digital service providers, as well as regulated electronic administration service providers, and central electronic administration service providers, as defined by this Act;

cc) services relating to electronic signatures and electronic seals, and generation of certificates relating to such services for persons working in protected positions, as specified by a separate law, and persons subject to national security vetting, as well as for organs involved in, or in the authorisation of, secret information gathering or using covert means;

cd) issuing encryption certificates for use by digital service providers, as well as regulated electronic administration service providers, and central electronic administration service providers, as defined by this Act, for persons working in protected positions, as specified by a separate law, and persons subject to national security vetting;

ce) verification of the validity of certificates issued pursuant to subpoints ca) to cd) through a real-time certificate status verification service;

d) other regulated electronic administration service to be provided as mandatory government service pursuant to a government decree issued on the basis of authorisation by this Act.

(2) In addition to those listed in paragraph (1), a law may also require other organs to provide certain regulated electronic administration services.

25. Electronic identification service provided as a mandatory government service

Section 46 (1) Electronic identification services that are provided as a mandatory government service shall be the following:

a) the service *eAzonosítás* (eIdentification); and

b) the *ügyfélkapu* (Client Gate) ensuring advanced two-factor identification.

(2) An identification service listed in paragraph (1) may be available to natural person users who are recorded in the register of personal data and addresses.

(3) A natural person user recorded in the register of personal data and addresses may use the identification service referred to in paragraph (1) b) until the activation by the user of the digital citizenship user profile referred to in section 11 (2); subsequently, only the identification service referred to in paragraph (1) a) shall be used by him.

(4) A natural person user who is recorded in the central aliens policing register or the register of foreign nationals using electronic administration shall use the identification service referred to in paragraph (1) b).

(5) A party using an electronic identification service provided as a mandatory government service shall be entitled to use, free of charge, an electronic registered delivery service integrally connected to the electronic identification service listed in paragraph (1), as specified in a decree by the Government, and the related storage.

(6) The rules on the client registration records and the entry into the records shall apply to the digital citizenship register with the derogations set out in section 12.

(7) Where a user is registered in accordance with paragraph (1) b), the digital citizenship register shall contain the public and confidential technical data required for carrying out identification, in addition to those listed in section 13 (1).

(8) The technological solution used for

a) verifying data;

b) acquiring data

recorded in the digital citizenship register that are requested by a digital service provider using an electronic identification service provided as a mandatory government service shall ensure that the organ keeping the digital citizenship register is notified only of querying the electronic identification service, without learning the identity of the addressee of the query. The technological solution shall transfer only the data request by the digital service provider and the data covered by the request and shall only verify the data provided by the digital service provider against the data kept in the digital citizenship register.

Chapter VII

CENTRAL ELECTRONIC ADMINISTRATION SERVICES

26. General rules

Section 47 (1) The Government shall provide the following central electronic administration services acting through a service provider designated by law:

a) register of the administrative settings of clients;

b) record validity register;

c) the service *eFizetés* (ePayment);

d) conversion of paper-based records to authentic electronic records;

e) conversion of electronic records to authentic paper-based records;

f) central identification agent;

g) custom front office, an online application customisable by the user, which provides a uniformly available option for identified users to make statements as necessary for electronic administration, perform procedural acts and other obligations, and use electronic administration services available to the user;

h) form submission service that allows, subject to electronic identification, users to fill in and submit to digital service providers electronic forms meeting the technical requirements set by an organ or a service provider specified by law;

i) the service *ePapír* (ePaper);

j) data link register.

k) role certification platform service;

l) automated administrative decision making system;

m) central electronic administration service specified in a decree of the Government.

(2) Where the use of a central electronic administration service is conditional upon registration, only an electronic identification service may be used for registration, unless provided otherwise by law. In the course of registration, an electronic identification service provider may transfer to the designated service provider personal data processed by the electronic identification service provider that are necessary for registration, subject to consent by the relying party.

(3) An Act or a government decree may make the use of a central electronic administration service mandatory.

(4) The general data processing rules as laid down in this Act shall apply to the processing of data, in the context of providing a central electronic administration service, by a service provider designated by the Government.

(5) Technology based on artificial intelligence may also be used in the context of supporting services.

(6) Where, under the law, the validity of a statement is conditional upon the signature of the user or the representative of the digital service provider, that signature may be substituted in the course of using the artificial intelligence-based system specified in a decree of the Government in accordance with the provisions of the decree of the Government.

(7) Where, in the course of using an artificial intelligence-based service, the digital service provider makes a statement via machine-based means through that service, the central electronic administration service provider shall act on behalf of the digital service provider.

(8) An Act or a government decree may specify the matters in which the use of all or any of the services referred to in paragraph (6) is prohibited.

27. Registration of the administrative settings of clients

Section 48 (1) With a view to facilitating electronic administration and providing various options for users, and respecting the instructions given by them in relation to electronic administration, the organ designated by the Government shall keep a register of the data content of administrative settings applied by users.

(2) When recording a data link entry of a new natural person into the data link register, the data controller of the data link register shall notify by electronic means the organ keeping the administrative settings of the client, for the purpose of creating an entry in the client settings register for processing the settings of that person.

(3) The organ keeping the client settings register shall generate, on the basis of natural identification data provided pursuant to paragraph (2), an internal identifier and assignment code for the link entry of a person; subsequently, it shall provide for the transfer of the link entry assignment code, encrypted using a method that can be reversed only by the organ keeping the client settings register, to the organ keeping the data link register, and shall thereafter delete all natural identification data.

(4) When registering a client setting concerning representation, the organ keeping the client settings register shall enter the representative into the register using a service that is based on the data link register, without storing any natural identification data of the representative or any identifier or identification code generated by another authority.

(5) The organ keeping the client settings register shall verify the right of representation.

(6) The organ keeping the client settings register shall provide data on the content of any administrative settings, including any data on authorisations granted by a user, only to digital service providers and supporting service providers. Digital service providers and supporting service providers shall confirm which identification codes or other identifiers they are authorised to use.

(7) When providing information on the contents of administrative settings, the registering organ may disclose, using the link register, to the requesting organ or service provider only identification codes and other data that the requesting organ or service provider is authorised to process.

(8) An Act or government decree may allow a digital service provider or a supporting service provider to report, in a manner specified by law, certain administrative settings of the user, as specified by law, to the organ keeping the client settings register for the purpose of entry into the register.

(9) Unless provided otherwise in an Act, the organ keeping the client settings register or a registration organ of the client settings register shall process personal data provided by a user, another organ, or a service provider referred to in paragraph (8) in the course of registering any administrative setting only for the purpose of registering the given administrative setting, until registration is completed.

28. Record validity register

Section 49 (1) Through the record validity register service, the service provider shall enable the relying parties to verify the authenticity and, where relevant data is available, content of authentic paper-based or electronic deeds in their possession.

(2) Parties using the record validity register service shall record in the record validity register certain data and parts of content, specified by the service provider, of the deeds they issue. The document validity register shall be available to the public, and any person may consult the register to verify data relating to a deed in his possession that is recorded in the register, and, if possible, also the validity of such a deed.

29. Conversion of paper-based records to authentic electronic records

Section 50 A deed produced by an organ designated by the Government on the basis of a record pursuant to the rules of the service for conversion of paper-based records to authentic electronic records shall have the same probative value as the original deed.

30. Conversion of electronic records to authentic paper-based records

Section 51 A deed produced by an organ designated by the Government on the basis of an electronic record pursuant to the rules of the service for conversion of electronic records to authentic paper-based records shall have the same probative value as the original deed.

Chapter VIII

DIGITAL CITIZENSHIP SERVICES

31. Digital framework services

Section 52 (1) Framework services accessible in the digital space shall be the following:

a) *eAzonosítás* (eIdentification);

b) *eAláírás* (eSignature);

c) *ePosta* (ePost);

d) *eDokumentumkezelés* (eDocument management);

e) *eFizetés* (ePayment).

(2) The digital framework services shall be provided by the digital citizenship service provider designated in a decree by the Government.

(3) The digital citizenship service provider shall provide the user with a framework application that ensures access to, and the use of, digital services, either separately or in an aggregated manner.

(4) A legal entity voluntarily undertaking to provide a digital service may use the digital citizenship framework services for its own digital services that are notified to, and authorised by, the digital services supervisory authority; for this purpose, the legal entity may connect to the digital framework application and the digital framework services. The technical, administrative, and accounting conditions for such connection are set out in a government decree.

(5) The provisions laid down in the Act on the general rules on taking up and pursuing service activities shall apply to the provision of a digital framework service and the framework application referred to in paragraph (3), with the derogations provided for under this subtitle and in a decree by the Government, accordingly.

Section 53 The service *eAzonosítás* (eIdentification) accessible as a digital framework service shall be an electronic identification service within the meaning of section 46, which shall use a biometric security function of a portable device of the user to increase the assurance level.

Section 54 (1) An electronic signature generated for a user using the service *eAláírás* (eSignature) accessible as a digital framework service shall qualify as a qualified electronic signature within the meaning of section 8, point 38.

(2) The service *eAláírás* (eSignature) shall be suitable for producing a private deed of full probative value and a public deed.

(3) A pseudonym shall not be indicated in the certificate associated with the service *eAláírás* (eSignature).

(4) The service *eAláírás* (eSignature) shall become available for use following activation in the national digital identity wallet.

(5) The digital citizenship service provider shall notify the trust service provider, using the digital citizen identifier, of the activation and deactivation of the user profile of a user, for the purpose of carrying out the tasks relating to the generation, verification and validation of the certificate associated with the service *eAláírás* (eSignature).

(6) The trust service provider providing the service *eAláírás* (eSignature) shall notify the digital citizenship service provider of the issuance and revocation of a certificate, and of the dates thereof.

(7) A user shall use the service *eAláírás* (eSignature) as a private person. The service *eAláírás* (eSignature) does not certify any attribute.

Section 55 (1) The service *ePosta* (ePost) available as a digital framework service shall provide the user with electronic storage corresponding to the electronic registered delivery service address, enable the sending of electronic documents, and certify successful or unsuccessful delivery and the downloading by the addressee of the document served.

(2) The digital citizenship service provider shall provide a storage, functionally separated according to the role of the user, for the sending, receipt and storage of electronic documents.

Section 56 The service *eDokumentumkezelés* (eDocument management) available as a digital framework service shall enable the production of authentic electronic documents. The services *eAláírás* (eSignature) and *eDokumentumkezelés* (eDocument management) may be provided also as an integrated service.

Section 57 (1) The service *eFizetés* (ePayment) available as a digital framework service shall enable users to fulfil their obligations to pay public burdens, fines and fees, as well as other payment obligations, (hereinafter jointly "payment obligation"), in the electronic space.

(2) Unless an Act or government decree provides otherwise, a natural person user may, and an economic operator user shall, fulfil their payment obligations by electronic means.

32. Life-event based services

Section 58 (1) Digital services falling within the functions and powers of an organ required to provide a digital service shall primarily be provided in a manner organised around life events.

(2) Live-event based services shall be specified by a government decree (hereinafter the "life-event catalogue").

(3) For digital services made available to economic operator users, services organised around business administration events may be developed, taking into account the operational characteristics of the organisation concerned.

(4) The provisions of the law relating to life events and life-event-based digital services shall apply also to business administration events and digital services supporting business administration events.

(5) In the course of designing and operating a life-event-based service, the service provider shall

a) decide on the conceptual directions and content of necessary developments;

b) design the life-event-based service, taking into account the recommendation by the professional contributor designated in the government decree referred to in paragraph (2);

c) develop the data connections and the most effective technical solutions that are required for a successful service on the part of the service provider, and request the establishment of the data connection referred to in paragraph (6) b) at the professional contributor;

d) determine the optimal procedure for matters connected in the context of a life event, and process data to the extent necessary;

e) make available the life-event-based service through the framework application or another digital administration platform.

(6) In the context of paragraph (5), a professional contributor shall

a) make a recommendation to the life-event service provider as regards the development of a new life event;

b) develop the data connections and the most effective technical solutions that are required for a successful service on the part of the professional contributor;

c) transform its administrative processes to the extent necessary for the development of the life-event-based service;

d) with the consent of the life-event service provider, initiate the amendment of laws relating to its functions at the member of the Government with the relevant functions, where necessary for the development of the life-event-based service.

(7) Within the framework of the cooperation under paragraphs (5) and (6), the life-event-provider may give guidance to the professional contributor in relation to the development of the life-event-based service, which shall be observed by the professional contributor.

33. National digital identity wallet

Section 59 The digital citizenship service provider shall provide a national digital identity wallet service, which enables a natural person user the use, both online and offline, of person identification data and certain attributes for using public and private services.

Section 60 The national digital identity wallet service shall enable a user to make arrangements in relation to

a) enabling the targeted sharing of his person identification data for identification and proving identity, or limited to what is necessary for the service used; and

b) sharing another attribute stored in the wallet other than the person identification data.

Section 61 (1) The following shall be deemed equivalent to presenting a physical official document proving identity or containing person identification data or attributes:

a) sharing an electronic attestation of attributes accessible within the framework of the national digital identity wallet service;

b) making available a data storage code for displaying the data content stored in a publicly certified register, within the framework of the national digital identity wallet service; and

c) sharing an authentic certificate digitally produced by the digital citizenship service provider in relation to the data content stored in a publicly certified register, within the framework of the national digital identity wallet service,

for the purpose of proving identity, person identification data or an attribute.

(2) An authorised person or organisation may verify data displayed from a publicly certified register on the basis of a data storage code that was made available in accordance with paragraph (1) b), for a purpose referred to in paragraph (1); in the event of a match, the identity, the person identification data, and the attributes shall be considered verified.

(3) By way of derogation from paragraphs (1) and (2), an attribute specified in a government decree may be proved in the framework of the national digital identity wallet service by presenting it through the framework application.

34. General rules of consent-based data provision

Section 62 (1) The digital citizenship service provider shall ensure that users holding an active user profile can make arrangements as regards the service provider transferring in the digital space a certain set of personal or other data recorded in state publicly certified digital registers and other electronic information systems.

(2) An arrangement referred to in paragraph (1) may cover

a) *ad hoc* data transfer; or

b) ensuring permanent data access.

(3) An arrangement referred to in paragraphs (1) and (2) may be made for organs connected to an aggregate service of the digital citizenship service provider.

(4) The digital citizenship service provider shall process an arrangement referred to in paragraphs (1) and (2) in the register of consents by the users for the purposes of data transfer, linked to the digital citizen identifier of the user.

(4a) The digital citizenship service provider may provide expert services for a fee to organs connecting to the aggregate service and the consent-based data provision in the course of connecting to and using the service.

(5) The Government shall, in a decree, specify the data registered by the digital citizenship service provider for the purposes of consent-based data provision, and lay down the rules on aggregate service provision, connection to the service, expert services available in the course of connecting to and using the service, fees for such expert services, and keeping the register of connecting organs.

35. User profile

Section 63 (1) User profile activation shall require the verification of identity. Identity shall be verified as follows:

a) without appearing in person, by means of

aa) remote identification; or

ab) an identity card fitted with a storage component; or

b) by means of pre-registration requiring appearance in person.

(2) The identification referred to in paragraph (1) may be used for requesting a signature certificate associated with the service *eAláírás* (eSignature) in accordance with Article 24 (1a) c) and (1b) d) of the eIDAS Regulation.

(3) Identification without appearing in person shall be in conformity with identification methods applicable to trust services that are prescribed by the law and provide equivalent assurance in terms of reliability to physical presence.

(4) In the course of remote identification, the digital citizenship service provider shall compare the natural identification data retrieved, by means of a video signal, from the official document used for verifying identity or its storage component, the facial image, the nationality, and the document identifier with data recorded in the central register in which the official document is recorded, and verify the validity of the official document. In the course of remote identification, the digital citizenship service provider shall compare the facial image of the user produced by means of a video signal with the facial image from the official document used for verifying identity or its storage component. The service referred to in section 12/B of the Facial Image Analysis Act may also be used to verify the identity of a user.

(5) In the course of identification using an identity card fitted with a storage component, the digital citizenship service provider shall compare the document identifier, the validity period, and the natural identification data retrieved, by means of the framework application, from the official document or the storage component with the data recorded in the central register in which the official document is recorded, and verify the validity of the official document.

(6) For the purposes of the verification of identity, the receipt referred to in paragraph (7), and the data transfer referred to in paragraph (13), the digital citizenship service provider

a) may receive the natural identification data, nationality, sex, and facial image of the person concerned, as well as data relating to the validity of the official document, and the document identifier of the official document, from the central register in which the official verification card suitable for verifying identity is recorded, on the basis of the document identifier obtained pursuant to paragraph (4);

b) may receive the natural identification data of the person concerned as well as data relating to the validity of the official document, and the document identifier of the official document, from the central register in which the official verification card suitable for verifying identity is recorded, on the basis of the document identifier obtained pursuant to paragraph (5).

(7) The digital citizenship service provider shall receive from the digital citizenship register the digital citizen identifier of the person concerned for the purposes of identifying the person concerned in the digital citizenship register on the basis of the natural identification data, verified in accordance with paragraph (6), and the document identifier, as well as the provision of the service *eAláírás* (eSignature). Where the organ keeping the digital citizenship register cannot establish the identity of the person concerned on the basis of the data provision referred to in section 12 (2), or the official document used to prove identity is invalid, registration shall not be permissible.

(8) In the course of a proceeding under paragraph (4), identification shall be considered successful if the data recorded in the register match, the official verification card suitable for verifying identity is valid, and the required threshold of match is reached.

(9) Should identification in accordance with paragraph (8) remain unsuccessful, the user may attempt identification also with assistance from an administrator of the digital citizenship service provider carrying out identification.

(10) Should identification in accordance with paragraph (7) be successful, the digital citizenship service provider shall transmit to the organ keeping the digital citizenship register the outcome of the identification, together with the natural identification data and nationality of the person concerned, as well as data relating to the official verification card suitable for verifying identity, for the purpose of activating the user profile. The organ keeping the digital citizenship register shall notify the digital citizenship service provider of the activation of the user profile. The notification shall include the digital citizen identifier of the person concerned.

(11) The digital citizenship service provider shall provide citizens with the option of digital citizenship pre-registration through the organ referred to in paragraph (12).

(12) Pre-registration may be requested in person

a) at any district office;

b) at the government office designated in accordance with the Act on the registration of personal data and address of citizens; or

c) at the organ maintaining the register under the Act on the registration of personal data and address of citizens,

subject to verification of the identity of the citizen.

(13) For the purpose of verifying identity in the course of pre-registration, the organ referred to in paragraph (12) may request from record-keepers the following as regards the user:

a) data listed in section 29 (2) and section 11 (1) n) of the Registration Act, and personal identifier;

b) data listed in section 8 (1) a) aa) to ad) and section 8 (1) b) ba) and bb) of Act LXXXIV of 1999 on the road traffic register; and

c) data listed in section 24 (1) a) to c), e) and f) of Act XII of 1998 on traveling abroad.

(14) After the identity of the user is verified, the digital citizenship service provider shall through the organ referred to in paragraph (12), provide the user with a code readable with the camera of a mobile device that contains the information confirming successful pre-registration (hereinafter the "pre-registration data"). Users shall store pre-registration data on their mobile device by means of the framework application. The digital citizenship service provider shall store an irreversible hash of the pre-registration data until registration, but for no longer than 6 months. The digital citizenship service provider shall notify the organ keeping the digital citizenship register of the successful completion of the registration.

(14a) Following the notification referred to in paragraph (14), the organ keeping the digital citizenship register shall notify the digital citizenship service provider of the activation of the user profile. The notification shall include the digital citizen identifier of the user.

(15) The digital citizenship service provider may provide the trust service provider providing the service *eAláírás* (eSignature) with the pre-registration data, which may be used by the trust service provider for the issuance of the signature certificate associated with the service *eAláírás* (eSignature).

Section 64 (1) The user may deactivate his user profile. Deactivation at the request of the user shall be permissible only through administration requiring appearance in person.

(1a) For the purpose of verifying identity in the course of the deactivation of digital citizenship, the organ referred to in section 63 (12) may request from keepers of the registers the following as regards the user:

a) data listed in section 29 (2) and section 11 (1) n) of the Registration Act, and personal identifier;

b) data listed in section 8 (1) a) aa) to ad) and section 8 (1) b) ba) and bb) of Act LXXXIV of 1999 on the road traffic register; and

c) data listed in section 24 (1) a) to c), e) and f) of Act XII of 1998 on traveling abroad.

(2) The organ keeping the digital citizenship register shall deactivate the user profile of a user in the event of removal from the register referred to in section 12 (2) with effect from the date of such removal.

(3) If paragraphs (1) and (2) apply,

a) the conditions for the reactivation of;

b) the legal effects of the deactivated status of

the user profile shall be established in a government decree.

(4) A user profile shall terminate upon the death of the user.

(5) If paragraph (3) applies, the organ keeping the digital citizenship register shall proceed in accordance with the provisions of section 14.

(6) The organ keeping the digital citizenship register shall notify the digital citizenship service provider of the deactivation of a user profile in accordance with paragraphs (1) and (2). The notification shall include the digital citizen identifier of the person concerned.

Chapter IX

THE USE OF CERTAIN SUPPORTING SERVICES BY THIRD-PARTY SERVICE PROVIDERS

Section 65 (1) A service, specified in an Act or a government decree, ensured by the Government that is

a) a digital framework service or a supporting service may be requested for the purpose of serving the public interest by an organ performing a public duty, which does not qualify as a digital service provider, under the conditions set out in a decree of the Government;

b) a digital framework service, a supporting service or another, IT, network or infrastructure public service may be requested, as a central state service provided to market participants, by an organisation not qualifying as a digital service provider, under to the conditions and with the derogations and limitations, in comparison to the original service, as set out in a decree of the Government.

(2) If a service referred to in paragraph (1) is provided, against remuneration, to market participants specified in an implementing decree of this Act, the market service provider may not claim any remuneration for the onward provision of services referred to in paragraph (1) in the course of providing services to other relying parties.

(3) If an electronic identification service provided by the Government or, subject to the derogations specified in a decree of the Government, a central state service provided to market participants of identical content is used, the market participant shall process the personal data that are indispensable for the use of the service in order to ensure the conduct and the success of identification process.

(4) The digital services supervisory authority shall supervise, in accordance with subtitle 38, compliance with the conditions under this chapter of supporting services and central state services provided to market participants (for the purposes of this section, hereinafter jointly the "Service") and the implementation of the rights and obligations prescribed in the laws relating to the Service, with the proviso that in the context of supervisory review, the Service shall be regarded as a regulated electronic administration service, the party using the Service shall be regarded as a digital service provider, and the person or organ communicating electronically with the party using the Service shall be regarded as a user.

(5) The provider of the Service may provide expert services to the relying party for a fee in the course of connecting to and using the service. The detailed rules on the expert service and on establishing the fee shall be determined by the Government in a decree.

Section 66

Chapter X

REGISTRATION OF FOREIGN NATIONALS USING ELECTRONIC ADMINISTRATION

36. Registration of foreign nationals using electronic administration

Section 67 (1) With a view to ensuring the security of electronic administration, the authentic electronic identification of users, and the use of certain electronic administration services, the organ designated by the Government shall keep a register of foreign natural persons who habitually reside in another country, do not have a registered domicile or place of residence in Hungary, and apply for registration voluntarily for the purpose of administering matters by electronic means (hereinafter "register of foreign nationals").

(1a) The register of foreign nationals shall officially certify data required for identification in the course of digital administration.

(2) A natural person who resides in another country and does not have a registered domicile or place of residence in Hungary may administer his matters falling with the scope of this Act by electronic means, even without registration pursuant to paragraph (1), provided that he

a) falls within the scope of the eIDAS Regulation, and identifies himself using an electronic identification means meeting the requirements specified in Article 6 (1) of the eIDAS Regulation; or

b) is entitled to do so under an international treaty.

(3) Natural person users shall appear in person before the registration organ designated by the Government in order to register. A proceeding conducted by the registration organ at an external site shall be considered equivalent to appearance in person, provided that the identity of the user can be verified as required by this section, under the same security conditions.

(4) When appearing in person, the registration organ shall identify a natural person on the basis of data indicated in a travel document suitable for verifying identity, as specified by a separate law, that is presented by the person concerned or, if the person concerned is a citizen of a Member State that is party to the Agreement on the European Economic Area, in a document suitable for verifying identity issued by the Member State. The registration organ shall verify the natural identification data of the natural person, as indicated on his presented document, against data recorded in

a) the register of personal data and addresses;

b) the central aliens policing register; and

c) the register of foreign nationals.

(5) The registration organ shall compare data received during the verification process with data indicated on the document presented by the natural person, and it shall determine whether the facial image on the document presented matches the person present.

(6) The registration organ shall verify, on the basis of the document identifier, whether the document presented by the user has already been used for registration in the register of foreign nationals. If it has, registration shall be denied.

Section 68 (1) If a natural person is not included in any of the registers listed in section 42 (2), and the facial image on the document presented matches the person present, the registration organ shall, recording the facial image and signature of the natural person applicant using the method specified in the relevant government decree, enter the natural person into the register of foreign nationals.

(2) The registration organ shall deny the registration of a client, and erase all recorded data irreversibly, if the data of the natural person user are already included in any of the registers referred to in section 42 (2), or if the deed presented by the user as proof of identity is invalid.

(3) The registration organ may use the data under section 42 (2) only for the purpose of determining whether the data match.

Section 69 (1) Registration in the register of foreign nationals shall terminate

a) upon the death of the natural person;

b) at the request of the natural person;

c) on the basis of a notification by the data link register if the data link entry generated for a registered person includes an encrypted link assignment code relating to a personal identifier or to an identifier used in the central aliens policing register;

d) upon the expiry of the validity of the official document used to verify identity during registration or, if that official document does not have a date of expiry, 50 years after registration.

(2) The register of foreign nationals shall contain, for a period of 5 years after the termination of registration, the facial image and signature of a natural person, as well as

a) his natural identification data if he appeared in person for identification during registration;

b) person identification data that were disclosed during registration and that identify him exclusively, in a situation not falling within the scope of point a);

c) the issuer, type, and validity period of the official document or means suitable for verifying identity used for identification;

d) sex and nationality of the natural person; and

e) the identifier of the official document or means referred to in point c).

(3) Data may be provided from the register of foreign nationals to an electronic identification service provider for the purpose of enabling the electronic identification service provider

a) to determine whether a given person is the same as a person included in its register;

b) to verify the identity of a given person for those requesting identification;

c) to provide data, as strictly necessary to identify a given person, to those requesting identification.

(4) For a purpose specified in sections 10/E and 10/F of the Means of Identification Act, data may be provided from the register of foreign nationals through the data link register if the data controller is authorised by an Act to process the data.

(5) An organ keeping the register referred to in paragraph (1) may disclose user data without the consent of the user to the following organs:

a) the court for the purposes of verifying the correctness of a statement of fact made in relation to a person involved in a proceeding pending before the court or the authenticity of data contained in a deed presented, conducting a criminal proceeding and enforcing a penalty or measure; or

b) an investigating authority, for the purposes of preventing or detecting a criminal offence, conducting a criminal proceeding, and enforcing a penalty or a measure;

c) the prosecution service, for the purposes of carrying out its tasks, as specified in the Act on the prosecution service, relating to the protection of public order and the supervision of legality, as well as preventing or detecting a criminal offence, conducting a criminal proceeding, and enforcing a penalty or a measure;

d) a national security service, for the purpose of carrying out its tasks;

e) a counter-terrorism organ within the meaning of the Act on the police for the purposes of preventing, detecting, and interrupting a terrorist act or any criminal offence committed in relation to a terrorist act, and performing its tasks relating to counter-intelligence, intelligence and priority personal and facility protection.

Section 70 (1) The organs referred to in section 69 (3) to (5) may request data from the register of foreign nationals free of charge.

(2) Data may be provided for an organ other than those specified in paragraph (1) in return for the payment of an administrative service fee, subject to consent from the user.

Chapter XI

SUPPORT AND SUPERVISION OF DIGITAL SERVICE PROVISION

37. Design and implementation of digital services

Section 71 With a view to implementing the objectives of this Act, the organisation designated in a decree by the Government shall publish the rules and recommendations relating to the design and implementation of digital and supporting services, provide methodological support for the performance of these activities, and continuously monitor the outcomes.

38. Supervision of digital services

Section 72 (1) The task of the digital service supervisory authority (hereinafter the "Supervisory Authority") shall be to supervise, coordinate and promote the implementation of the right to digital citizenship and to the use of digital services, and the provision of digital services. The Supervisory Authority shall be designated by the Government in a decree.

(1a) The Supervisory Authority shall act as the national competent authority responsible for the application of Regulation (EU) 2024/903 of the European Parliament and of the Council and, as single point of contact, carry out the tasks listed in Article 17 (2) of Regulation (EU) 2024/903 of the European Parliament and of the Council.

(2) Acting within its functions provided for under paragraph (1), the Supervisory Authority shall supervise, in particular, the following:

a) digital services provided by a digital service provider;

b) supporting services;

c) digital citizenship services; and

d) compliance with the provisions of this Act and of the laws issued for its implementation relating to the services listed in points a) to c) and to the cooperation obligation in connection with those services, and shall take action in the event of a breach.

(3) In particular, the Supervisory Authority, acting within its functions provided for under paragraph (1) and in accordance with the provisions of this Act and the laws issued for its implementation,

a) shall record in the life-event catalogue the digital services available to the user, the matters categorised by life events, and the applications ensuring the integrated management of matters, as well as the digital service providers;

b) shall grant authorisation to, and register, legal entities who voluntarily subject themselves to this Act;

c) may launch a supervisory review upon notification by the user, except in cases specified in a law issued for the implementation of this Act;

d) may launch a supervisory review *ex officio* if it is likely, including on the basis of an anonymous notification, that a digital service provider, an organisation providing supporting services or an organisation providing digital citizenship services breaches its obligations, or the rights of users, set out in this Act;

e) shall perform the authority and supervisory tasks relating to the supervision of the implementation of provisions of laws laying down the requirements for state applications on which digital service provision is based as well as the requirements for digital service provision, and take action in the event of a breach;

f) shall conduct a coordination proceeding *ex officio* or upon request;

g) shall carry out, for supporting services and digital citizenship services, the authority supervision of the services pursuant to the Act on the general rules on taking up and pursuit of service activities.

(3a) Acting within its functions provided for in paragraph (1a), the Supervisory Authority shall, in particular, support the assessment procedure within the meaning of Article 3 of Regulation (EU) 2024/903 of the European Parliament and of the Council to be carried out by a public sector body, in accordance with the provisions of this Act and the law issued for its implementation.

(4) The Supervisory Authority shall conduct an administrative audit to check compliance with the requirements set out by this Act and the laws issued for its implementation.

(5) In the course of supervisory review, the notifier shall not exercise the right of a party as provided for under the Act on the Code of General Administrative Procedure, and shall not have the right to seek legal remedy against an authority decision adopted in an authority proceeding launched *ex officio*. The Supervisory Authority shall inform the notifier of the launch, and the outcome, of the supervisory review. Should the Supervisory Authority not launch a proceeding upon a notice, it shall, without delay, inform the notifier accordingly, without being obliged to give reasons.

(6) Where the Supervisory Authority establishes that a digital service provider, a supporting service provider, or the digital citizenship service provider (for the purposes of this section, hereinafter the "supervised organisation") breached the rules laid down in this Act or the implementing decrees to this Act,

a) as a legal consequence,

aa) it may, setting a time limit, require the supervised organisation to eliminate the errors and deficiencies identified;

ab) it may request the entity exercising disciplinary powers to establish the disciplinary liability, and liability for damages, of the person responsible for the implementation of digital services at the supervised organisation;

ac) it may make the provision of the digital service by the supervised organisation subject to conditions, restrict it, or suspend it from the date on which the decision reaches administrative finality until the lawful situation is restored, but for no longer than 12 months;

ad) it may order that budgetary funds shall no longer be allocated for the state operation and development of applications on which the provision of digital services is based;

b) as an administrative sanction,

ba) it may revoke, for an organisation voluntarily undertaking digital service provision, the licence of the organisation for digital service provision;

bb) it may impose a fine in an amount specified by the Government in a decree.

(7 The legal consequences and the administrative sanctions referred to in paragraph (6) may be imposed also jointly.

(8) The Supervisory Authority shall impose a fine if

a) the Supervisory Authority applied any of the legal consequences listed in paragraph (6) a) against the supervised organisation without result;

b) the infringement affects a wide range of users and causes a significant harm to interests or risk of damage;

c) the infringement caused a significant disadvantage to one or more users.

(9) If paragraph (8) applies, warning shall not be applied as an administrative sanction.

Section 73 (1) When providing services, a digital service provider, a supporting service provider, and the digital citizenship service provider shall proceed in compliance with the requirements set out in this Act and the implementing decrees of this Act; the Supervisory Authority shall supervise such compliance and take action in the event of a breach.

(2) Any contract relating to the development, upgrade and operation of applications on which the provision of digital services is based that is concluded in circumvention or violation of the rules of this Act and its implementing decrees shall be null and void.

PART FOUR

IT COOPERATION OF DIGITAL SERVICE PROVIDERS AND OTHER ORGANISATIONS

Chapter XII

THE FUNDAMENTAL REQUIREMENTS OF COOPERATION

39. Application of the rules on cooperation

Section 74 (1) With the exceptions provided for under paragraph (2), the rules laid down in this Part shall apply to communication and information transmission between digital service providers and organs performing a public duty designated by the Government (hereinafter jointly "cooperating organs"), and administration of matters, and IT cooperation, as provided for by this Act, in proceedings, involving any information transmission between cooperating organs, in their capacity as such, as required or permitted by this Act or any other law.

(2) The rules relating to joining and operating the single digital gateway that are required for implementing Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012 shall be laid down in a government decree.

(3) This Part shall not apply to

a) legislative procedures;

b) preparation of decisions by the Government;

c) election procedures and the preparation and holding of referendums;

d) transmission of data and records, or provision of data from the registers, of national security services or the National Security Authority, and their proceedings;

e) internal registers and draft decisions of cooperating organs;

f) subject to the exceptions provided for under this Act, procedures for granting access to data that are not public under the Act on the right to informational self-determination and on the freedom of information, and to records containing such data, of cooperating organs, that are used to support decision-making;

g) unless provided otherwise in an Act, transmission of classified data and records containing classified data;

h) relations governed by civil law between cooperating organs;

i) transfer of public documents to archives; and

j) handover-acceptance procedures relating to legal succession of cooperating organs under public or private law.

(4) With respect to any communication, information transmission, and administration of matters regulated by directly and generally applicable mandatory legal acts of the European Union, the provisions laid down in this Part shall not apply to the issues regulated by such legal acts. A law may derogate from the provisions of this Act to an extent and in a way that is necessary to implement a mandatory legal act of the European Union.

40. The fundamental principles of cooperation

Section 75 (1) In situations specified in this Act, a cooperating organ shall obtain from another cooperating organ by electronic means information that is necessary for handling a digital service (for the purposes of this Part, hereinafter the "matter") or performing its task and that was generated at, or has already been obtained by, the other cooperating organ, or a decision or statement of the other cooperating organ that is necessary for administering a matter.

(2) By way of derogation from paragraph (1), the digital citizenship service provider shall obtain data specified in the life-event catalogue by means of information transmission.

(3) Cooperating organs shall communicate with each other by electronic means, unless prohibited by an Act.

(4) Cooperating organs shall design their electronic information systems, and develop their existing electronic information systems, in such a manner that they are suitable, in line with the requirements laid down in this Act, for the purposes of their IT cooperation as required under this Act (hereinafter "IT cooperation").

(5) In a matter launched at the request or initiative of a client, the digital service provider shall transfer personal data available to it that is necessary to administer the matter to the digital service provider, which shall process it to the extent necessary and sufficient for administering the matter, if the digital service provider informed the client, in a manner meeting applicable requirements, about all material circumstances of data processing.

Chapter XIII

GENERAL RULES OF IT COOPERATION

41. Sources of information

Section 76 (1) If a cooperating organ is aware that a piece of information it is not in possession of but needs for administering a pending matter or carrying out a task is available from a primary source of information referred to in paragraph (3), it shall obtain the relevant piece of information from the primary source of information by electronic means, provided that the cooperating organ is authorised by an Act to process that piece of information if it constitutes personal or classified data, and that it is not prohibited from doing so by an Act.

(2) A cooperating organ shall obtain a piece of information referred to in paragraph (1) from a primary source of information by means of an information transmission service ensuring automated transfer, provided that it is available, and it is not prohibited from doing so by an Act.

(3) A piece of information shall be considered available from a primary source of information if

a) it is recorded in a publicly certified register;

b) it is not recorded in a publicly certified register, but it was generated at a cooperating organ; or

c) it is identified as such by law, with reference to the primary source of information.

(4) A cooperating organ shall be presumed, for the purposes of paragraph (1), to be aware of a piece of information being available from a primary source of information in the following cases:

a) in a situation described in paragraph (3) a) or c);

b) if the piece of information was generated at a cooperating organ;

c) if the user or the cooperating organ acting in the matter informed it accordingly, with reference to the piece of information and the primary source of information.

(5) Unless prohibited by an Act, a cooperating organ shall obtain a piece of information from a primary source of information by electronic means if there is any doubt regarding the accuracy or validity of a piece of information available to it.

Section 77 (1) If a piece of information that is not available to a cooperating organ is needed for administering a pending matter or carrying out a task cannot be obtained from a primary source of information, but the cooperating organ is aware that it is available from a secondary source of information, it shall obtain the piece of information from the secondary source of information by electronic means, provided that the cooperating organ is authorised by an Act to process that piece of information if it constitutes personal or classified data, and that a law does not provide otherwise.

(2) A piece of information shall be considered available from a secondary source of information if

a) it was obtained by a cooperating organ from a primary source of information; or

b) it was not generated at a cooperating organ, and it was obtained by a cooperating organ from an organ other than a cooperating organ.

(3) A cooperating organ may obtain from a secondary source of information a piece of information that is available from a primary source of information also if it is ensured that the information available from the secondary source of information matches the information available from the primary source of information, provided that all the other conditions specified in this section are met.

(4) Where a proceeding in accordance with paragraphs (1) to (3) or section 76 takes a disproportionately long time or if establishing the required technical conditions does not serve the principle of cost-effectiveness, the digital citizenship service provider may obtain information also from another source of information.

42. The methods of transferring information

Section 78 (1) A cooperating organ specified in a government decree shall set up, and make available to other cooperating organs, an information transmission service that ensures the automated transfer of pieces of information specified in a government decree.

(2) In place of using information transmission, a cooperating organ may also make pieces of information available to it, that may or are to be transmitted under a law, available to another cooperating organ by electronic means, provided that the necessary IT conditions are met. If service has any legal consequence by law, or if a piece of information is to be provided within a time limit specified by law, the cooperating organ providing the information shall inform the other cooperating organ once the piece of information is made available.

Chapter XIV

SUPPORTING SERVICES USED IN THE COURSE OF COOPERATION

Section 79 (1) With a view to facilitating cooperation, a cooperating organ may use supporting services, as specified in Chapters VI and VII and in the implementing decree of this Act, in the course of cooperation and in its internal electronic administration procedures.

(2) In the course of any use referred to in paragraph (1), provisions laid down in Chapters VI and VII shall apply as appropriate, in line with the rules on data processing.

(3) In addition to services listed in section 47, the Government shall, through the service provider designated by a law, provide a central government service bus as a central electronic administration service, in the framework of which

a) the service provider ensures secure conditions for information transmission by connecting the information transmission services of information systems used by cooperating organs and other organisations connecting to the service voluntarily or, otherwise, as an information transmission service; and

b) in relation to data transfers of the information systems of connected cooperating organs that contain personal data, it provides a one-stop-shop information service to support the provision of information regarding the transfer of the personal data of the data subjects.

(4) An Act or a government decree may make mandatory the use of a central electronic administration service also in the course of such cooperation.

(5) The Government shall provide the legal entities listed in section 9 (2) with the supporting services required for cooperation and internal electronic procedures free of charge.

PART FIVE

CONNECTION BETWEEN THE DIGITAL SPACE AND THE SERVICE PROVIDERS

Section 80 (1) The following economic operators shall qualify as an organisation required to ensure a digital service:

a) an economic operator providing a service classified as a waste management public service subactivity under the Act on waste;

b) a district heating provider within the meaning of the Act on district heating;

c) with respect to users relying on the universal service it provides, a holder of a universal gas service provision licence, and a gas distribution licence holder;

d) a water utility service provider within the meaning of the Act on water utility services;

e) a provider of a service for the systematic retrieval, collection, transport and deposit of domestic waste water collected by means other than public utility services;

f) a provider of a chimney-sweeping service;

g) a provider of a universal postal service;

h) with respect to users relying on the universal service it provides, a holder of a universal electricity service provision licence, and an electricity distribution licence holder;

i) a credit institution and a financial undertaking within the meaning of the Act on credit institutions and financial undertakings;

j) a payment institution, an electronic money institution, and the institution operating the Postal Clearing Centre, within the meaning of the Act on certain payment service providers;

k) an insurance institution and a reinsurance institution within the meaning of the Act on the insurance business;

l) an investment firm, and a commodity exchange service provider, within the meaning of the Act on investment firms and commodity exchange service providers, and on the regulations governing their activities;

m) an economic operator carrying out an activity falling within the scope of the Act on Voluntary Mutual Insurance Funds, the Act on private pension and private pension funds, or the Act on occupational pension and its institutions;

n) a provider of a mutual insurance association service within the meaning of the Act on the insurance business;

o) an electronic communications service provider providing an individual subscription service within the meaning of the Act on electronic communications.

(2) The rules on the legal entities listed in section 9 (2) shall apply to an economic operator referred to in paragraph (1) a), b), d), f) or g) that issued an average of at least 50 000 invoices per month for its services in the year preceding the year in question, with the derogation that, from among the framework services, it shall provide the framework services listed in section 52 (1) a) and b).

(3) By way of derogation from Parts THREE and FOUR, an economic operator specified in paragraph (1) a), b), d), f) or g), of which the number of invoices issued does not reach the threshold set out in paragraph (2), shall be required to provide only the framework services listed in section 52 (1) a) and b) in the course of the provision of its own services, in addition to or in place of its own service with the same function.

(4) By way of derogation from Parts THREE and FOUR, an economic operator specified in paragraph (1) i) to n) shall be required to provide only the framework services listed in section 52 (1) a) and b) in the course of the provision of its own services, in addition to or in place of its own service with the same function.

(5) The rules on the legal entities listed in section 9 (2) shall apply to an economic operator specified in paragraph (1) c), e) or h) of which the services were used by not less than 50 000 natural person users in the year preceding the year in question, with the derogation that, from among the framework services, it shall provide the framework services listed in section 52 (1) a) and b).

(6) By way of derogation from Parts THREE and FOUR, an economic operator specified in paragraph (1) o), of which the services were used by not less than 50 000 natural person users in the year preceding the year in question, shall be required to provide only the framework services listed in section 52 (1) a) and b) in the course of the provision of its own services, in addition to or in place of its own service with the same function.

Section 81 (1) In relation to digital citizenship services to be provided as mandatory in accordance with section 80 (2) to (6), and digital citizenship services and supporting services used beyond that, an organisation required to ensure a digital service shall be required to comply with the following conditions:

a) registration by the digital citizenship service provider, by means of electronic communication;

b) acceptance of service conditions set out by the digital citizenship service provider

c) compliance with technical requirements set out by the digital citizenship service provider;

d) compliance with cybersecurity requirements for its electronic information systems; and

e) payment of administrative service fee to the digital citizenship service provider.

(2) Organisations listed in section 80 (1) a) to h) and o) shall fulfil the condition set out in paragraph (1) d) by ensuring compliance with the cybersecurity requirements set out in the Act on the cybersecurity of Hungary, and by carrying out a cybersecurity audit.

(3) For organisations listed in section 80 (1) i) to n), the condition listed in paragraph (1) d) shall be fulfilled by using an IT system that ensures that the components are closed, and prevents unauthorised access to the IT system and any undetected modification thereof. The IT system shall comply with also the general information security closed-system requirements. To this end, organisations listed in section 80 (1) i) to n) shall ensure compliance with general information security closed-system requirements by means of administrative, physical, and logical measures.

(4) Evidence of compliance with the requirements set out in paragraph (3) shall be provided by means of a certificate relating to the IT system, that is issued by an external expert (hereinafter the "certifying organisation"). Requirements relating to certifying organisations, certification, and the maximum fee, calculated without value added tax, of the certification procedure shall be determined by the Government in a decree.

(5) A certifying organisation and its subcontractor shall be authorised to process data, including personal data and trade secrets, as required for certification, that are processed by an organisation listed in section 80 (1) i) to n), for the purpose of assessing compliance with the requirements to be certified, to the extent necessary for the conduct of the certification proceeding, and until the completion of the certification proceeding; such data shall not be transferred to third parties.

(6) A certifying organisation and its subcontractor shall specify in regulations the positions the holders of which may access, and learn the content of, trade secrets in the course of a certification proceeding. Employees participating in a certification proceeding shall be subject to an obligation of confidentiality as regards any trade secret they became aware in the course of the proceeding, even after the termination of their legal relationship with the certifying organisation.

(7) In addition to the conditions set out in paragraph (1), a government decree may set further admission conditions.

(8) An organisation required to ensure a digital service shall, in compliance with the requirements set out in paragraphs (1) to (7), continuously ensure, throughout the full period of service provision, compliance with the requirements of framework services. The Government shall specify in a decree the manner in which the fulfilment of the conditions is to be continuously ensured and in which it is to be certified.

(9) An organisation required to ensure a digital service shall ensure the use of framework services for users without compensation and without charging any other fee.

(10) The digital citizenship service provider may provide, to organisations referred to in section 80 (1), expert services in the course of connecting to and using a service, in the context of framework services. The detailed rules on the expert service and on establishing the fee shall be determined by the Government in a decree.

PART SIX

ON TRUST SERVICES

Section 82 (1) The rules in this Part shall apply to the following:

a) trust service providers, within the meaning of the eIDAS Regulation, established in Hungary, and trust services provided by them;

b) parties relying upon the trust services referred to in point a).

(2) The provisions laid down in this Part shall not apply to trust services that are used exclusively within closed systems pursuant to Article 2 (2) of the eIDAS Regulation.

Chapter XV

GENERAL CONDITIONS FOR PROVIDING TRUST SERVICES

43. Taking up the provision of trust services

Section 83 (1) Trust service providers established in Hungary shall notify their intent to take up the provision of trust services to the trust service supervisory body using the standard electronic form of the trust service supervisory body.

(2) Before launching a qualified trust service, the notification under paragraph (1) shall be submitted by the trust service provider at least 90 days before taking up the provision of the trust service.

(3) The trust service provider shall attach to the notification the records specified in an implementing decree of this Act.

(4) The trust service supervisory body shall assess the notification referred to in paragraph (1) and send the conformity assessment report referred to in Article 21 (1) of the eIDAS Regulation that is attached to the notification of the qualified service, to the competent authority for statement of a specialist authority. The trust service supervisory body shall register notifiers that comply with the requirements under the law and with the eIDAS Regulation, and provide for their inclusion in a trusted list within the meaning of Article 22 of the eIDAS Regulation.

(5) A trust service provider shall notify the trust service supervisory body of any change concerning its operation or the provision of trust services as compared to data entered into the register based on notifications.

(6) A trust service provider providing qualified trust services shall notify the trust service supervisory body about any planned change to trust service provision, at least 30 days before the introduction of the change.

(7) Notifications and applications relating to trust services shall be submitted to the trust service supervisory body directly.

44. Service contracts and requirements concerning the provision of trust services

Section 84 (1) A trust service provider and a trust service client shall enter into a service contract regarding the provision of trust services.

(2) Before concluding the contract, the trust service provider shall, in addition to providing all information required under the eIDAS Regulation inform trust service clients whether the trust service qualifies as a qualified trust service.

(3) In addition to the provisions of paragraph (2), a trust service provider shall also provide trust service clients with any information specified by the implementing decree of this Act, and it shall also make accessible to them any data or documents specified in this Act.

(4) Only persons without a criminal record who are not subject to disqualification from a profession, excluding them from providing trust services, may act as a natural person providing qualified trust services, and as an executive officer, manager, or employee of a legal person or an organisation without a legal personality operating as a qualified trust service provider.

(5) Detailed provisions concerning service contracts and other conditions of providing trust services (in particular trust service policies and service policies) shall be laid down in an implementing decree of this Act.

(6) A trust service provider may provide its trust services subject to different conditions, including, in particular, different rules on liability or applying different trust service policies; however, the trust service client shall be notified of any limitations prior to contract conclusion.

(7) After concluding a contract, the trust service provider shall provide its trust service client with a copy of the service contract, as well as the trust service policy and the service policy on a durable data-storage medium or in a downloadable format.

45. Verification concerning certificates issued through trust services

Section 85 (1) Any data contained in a certificate issued by a trust service provider shall be true, unless it is clear from the certificate itself that the data included was not verified by the trust service provider (in particular when a pseudonym is used). To this end, a trust service provider shall verify all data to be included in a certificate; in particular and depending on the content of a certificate, the trust service provider shall verify the identity of the certificate subject, the authenticity of any identification data used to verify identity, including the verification of that data against relevant data, if any, recorded in a publicly certified or other central register, the right of representation of the representative acting for the certificate subject before the trust service provider, the subsistence of the right of representation to be recorded in the certificate, the right to dispose of the domain to be indicated in the certificate, the right to dispose of the IP address to be indicated in the certificate, the existence of the organisational unit to be included in the certificate, and the right to exercise the regulated profession to be included in the certificate, if specified.

(2) With regard to qualified trust services, a trust service provider shall verify identity pursuant to Article 24 (1) of the eIDAS Regulation, with the proviso that the obligations provided for under paragraphs (3) to (8) shall be considered requirements under national law as referred to in the same paragraph of the eIDAS Regulation. With regard to non-qualified trust services, a trust service provider shall verify identity in a manner specified in Article 24 (1) of the eIDAS Regulation, and according to the obligations provided for under paragraphs (3) to (8), with the proviso that, in addition to a certificate of a qualified electronic signature or of a qualified electronic seal referred to in Article 24 (1) (c), it may also accept an advanced electronic signature or electronic seal.

(3) If a trust service provider intends to verify the identity of a natural person certificate subject through physical presence or equivalent means of identification, it shall, where the natural person falls within the scope of the Registration Act, do so on the basis of an official verification card suitable for verifying identity within the meaning of the Registration Act.

(4) If a trust service provider intends to verify the identity of a natural person certificate subject, who does not fall within the scope of the Registration Act, through physical presence or equivalent means of identification, it shall do so primarily on the basis of a travel document within the meaning of the Act on the entry and residence of persons having the right of free movement and residence or the Act laying down the general rules on the entry and residence of third-country nationals.

(5) If a trust service provider verifies the identity of a person pursuant to paragraph (4) through physical presence or equivalent means of identification outside the territory of Hungary, and the natural person certificate subject does not hold any of the travel documents specified in the laws referred to in paragraph (4), the trust service provider may verify his identity only on the basis of reliable official documents or other records, as specified in the authentication policy, with regard to which the trust service provider is able to demonstrate toward the trust service supervisory body that, for the purpose of establishing and verifying the identity of a person, the reliable official document or other record specified in the authentication policy affords the same degree of certainty as the means referred to in paragraph (4).

(6) If a trust service provider verified the identity of a natural person certificate subject pursuant to paragraph (3), it shall be obliged also to verify the validity of, and all data indicated on, the official verification card used to verify identity against the appropriate publicly certified official register.

(7) If a trust service provider verified the identity of a natural person certificate subject pursuant to paragraph (4) or (5), it shall also verify against the respective central registers the validity or authenticity of, and all data indicated on, the official document or other record referred to in paragraph (4) or (5) that is used as proof of identity. If such a register is not available or is not accessible by the trust service provider, or the costs of access and verification are disproportionately high, the trust service provider shall record this fact, and shall take a decision on the basis of other available evidence on whether to issue the given certificate to the certificate subject.

(8) If the certificate subject is an entity other than a natural person, the trust service provider shall verify at least the full name and unique identifier, as indicated in the certificate, of the certificate subject. Where the certificate subject is a person incorporated in Hungary, the trust service provider shall verify the correctness and timeliness of such data on the basis of the content of a relevant publicly certified register; if such a publicly certified register does not exist, the verification shall be carried out on the basis of the public deed certifying incorporation, and, in other respects, the provisions laid down in paragraph (5) shall apply to the verification.

(9) If a representative acts on behalf of a certificate subject before a trust service provider, or where the certificate includes any full or partial right of representation, or any legal relationship that may also be construed as such (hereinafter jointly “right of representation”), the trust service provider shall, before issuing the certificate, verify the subsistence and scope, as indicated in the certificate, of the right of representation against a law, a publicly certified register, instrument of incorporation or, in the absence of such, authorisation, and record the result of the verification.

Section 86 (1) Other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence shall be determined by the Government in a decree.

(2) If the other identification method under paragraph (1) is based on making an audio-visual recording, the trust service provider shall record, and retain for the period referred to in section 88 (1), in a retrievable manner, as an audio-visual recording, in a manner the excludes the deterioration of the quality of the recording, the full communication between the trust service provider and the natural person in the course of identification by means of video technology, as well as the detailed information provision to the natural person as regards identification by means of video technology, and the express consent by the natural person.

(3) If paragraph (2) applies, the trust service provider shall be entitled to store the image recording of the official document confirming the identity of the natural person for the period under paragraph (2).

46. General obligations concerning certificates issued through trust services

Section 87 If a certificate issued by a trust service provider through a trust service also certifies a right of representation,

a) the trust service provider shall notify the represented person without delay of the issuance of the certificate;

b) the trust service provider shall withdraw, upon termination of the right of representation or at the request of the representative or the represented person, the certificate indicating the subsistence of the right of representation,

c) the trust service provider may indicate a pseudonym in the certificate only with the consent of the represented person.

Section 88 (1) A trust service provider shall retain all available information relating to each certificate, including information on the generation of the certificate, as well as all related personal data, for at least 10 years from the expiry of the certificate. If a relying party, an authority, or the court notifies a trust service provider of a legal dispute launched concerning the correctness or validity of any data included in a certificate, the trust service provider shall be required to fulfil its retention obligation until the legal dispute is resolved with final and binding effect, even if such resolution takes place more than ten years after the expiry of the certificate. Until the expiry of the retention period, a trust service provider shall also provide means to determine the content of a certificate issued.

(2) A trust service provider may also fulfil its retention obligation by means of a qualified archiving service.

(3) In addition to the registers referred to in Article 24 (4) of the eIDAS Regulation, the trust service provider issuing a certificate shall, where the trust service provider allows the suspension of a certificate under the given trust service, also keep information on any suspension of the certificates issued by it continuously accessible.

Section 89 (1) A trust service client shall notify the trust service provider without delay about

a) any change to person identification data indicated in the certificate that are required for identification, to data of the authorised representative and the represented person, where the certificate was issued in relation to the representation of another person, and to any other data indicated in the certificate;

b) any irregularity detected regarding the trust service or the certificate, as defined in law, a service contract, or a service policy, or any other event affecting the trust service, including in particular any possibility of use by an unauthorised person of a cryptographic or other security device provided by the trust service provider that is required for the use of the trust service;

c) the launch of any legal dispute concerning the trust service.

(2) A trust service client or a relying party certified in a certificate pursuant to section 85 may request a certificate to be revoked or, where the trust service provider allows the suspension of a certificate in the context of the given trust service, suspended.

47. Suspension and revocation of certificates issued through trust services

Section 90 (1) With regard to a certificate issued by a trust service provider through a trust service, the trust service provider may decide to allow suspension affecting the validity of the certificate in situations specified in the authentication policy, service policy, or service contract.

(2) Where a trust service provider allows the suspension of a certificate, it shall suspend the validity of the certificate, and publish a reference to the suspension, including the exact period of suspension, in its register without delay

a) at a request of a person referred to in section 89 (2);

b) if it becomes aware of any irregularity concerning the service, as defined by a law, a service policy, or a service contract;

c) if there is reason to believe that the data included in the certificate is incorrect;

d) if ordered by the trust service supervisory body in a decision with administrative finality.

Section 91 (1) A trust service provider shall revoke a certificate and publish a reference to the revocation in its register without delay

a) at the request of a person referred to in section 89 (2);

b) if it becomes aware of any irregularity concerning the service, as defined by a law, a service policy, or a service contract, that cannot be remedied by suspending the certificate, or where the service provider does not allow the suspension of the certificate;

c) if it becomes aware that data included in the certificate is incorrect;

d) if ordered by the trust service supervisory body in a decision with administrative finality;

e) if the provision of the given trust service is discontinued.

(2) The revocation of a certificate by a trust service provider may not concern a period before the date of the publication of the revocation.

(3) The trust service provider shall specify in its service policy or service contracts the legal consequences of revoking a certificate before expiry.

(4) If a certificate not covered by Article 28 (4) of the eIDAS Regulation is revoked, it shall lose validity upon revocation.

Chapter XVI

DISCONTINUATION OF TRUST SERVICE PROVISON

Section 92 (1) If a trust service provider intends to discontinue the provision of a trust service, it shall notify accordingly the trust service supervisory body, its trust service clients, and all relying parties other than trust service clients indicated in its issued and yet unrevoked electronic signature and seal certificates, at the latest, upon the discontinuation of the trust service provision or, where the trust service provider is a qualified trust service provider, at least 90 days before discontinuation.

(2) If the trust service provider continues to provide any other trust service, it shall keep continuously available its registers related to the trust service to be discontinued that are already available to the public; in particular, it shall ensure access to the registers referred to in section 88 (3).

(3) If a trust service provider discontinues all trust service provision, the notification referred to in paragraph (1) shall specify a trust service provider (hereinafter "substitute trust service provider") that is to ensure access to the registers referred to in paragraph (2) even following the discontinuation of the trust service activities.

(4) If the trust service to be discontinued is a qualified trust service, only a trust service provider registered with the trust service supervisory body as a qualified trust service provider with respect to the same trust services may act as substitute trust service provider.

(5) Once a notification under paragraph (1) is given, the trust service provider shall not issue any new certificate in relation to the trust service concerned, and it shall revoke all certificates issued and not yet revoked at least 20 days before the discontinuation of the activity.

(6) A trust service provider shall disclose to its substitute trust service provider all registered data to which access is to be ensured, as well as all data relating to revoked certificates, including personal data.

Section 93 (1) If a trust service provider fails to perform an obligation provided for under section 92 (2) or (3), the trust service supervisory body shall order all certificates issued by the trust service provider to be revoked, it shall have a reference to the order published, and it shall designate a substitute trust service provider. All costs incurred by the trust service supervisory body in this context shall be reimbursed by the trust service provider discontinuing its trust service activities within 15 days after receipt of the corresponding notice from the trust service supervisory body. If a trust service provider discontinuing its trust services activities fails to reimburse such costs within the time limit, the trust service supervisory body may use, to recover its expenditures, the financial security provided for such purposes by the trust service provider under the law.

(2) Where a qualified trust service is concerned, the trust service supervisory body shall designate primarily a qualified trust service provider as a substitute trust service provider.

(3)

(4) If a liquidation, winding-up, or compulsory strike-off proceeding is instituted against a trust service provider, the trust service provider shall notify without delay the trust service supervisory body about the proceeding and the identity of the liquidator or winding-up administrator. During the period of the proceeding, the trust service supervisory body may request information from the liquidator, the winding-up administrator, or the company registration court conducting the compulsory strike-off proceeding about the progress of the liquidation, winding-up, or compulsory strike-off proceeding. If the trust service provider fails to perform its obligations provided for under section 92 (1) and (2) before submitting its closing balance sheet, the trust service supervisory body shall designate a substitute trust service provider.

(5) If a trust service provision is discontinued, the trust service supervisory body shall deregister the trust service; if a trust service provider is terminated, the supervisory body shall deregister all registered trust services provided by the trust service provider concerned.

Chapter XVII

THE OBLIGATION OF TRUST SERVICE PROVIDERS TO PROVIDE DATA

Section 94 (1) For the purposes of conducting a criminal proceeding for a criminal offence committed by abusing a trust service provided by a trust service provider, or in the interest of national security, the trust service provider shall provide the investigating authorities, the prosecution service, the court, the national security services, and the counter-terrorism organ within the meaning of the Act on the police with data confirming the identity of the person concerned and data verified pursuant to section 85 free of charge, provided that the conditions for data request are met. The data transmission shall be recorded; the trust service provider shall not inform the relying party about the data transmission.

(2) A trust service provider shall perform its obligations provided for under paragraph (1) without delay, and it may not apply any further condition regarding the data transfer; in particular, data transfer shall not be made conditional upon reaching any agreement on the costs of data provision, or on advancing any such costs.

(3) In the course of a civil action or a non-contentious proceeding concerning the validity of a certificate, a trust service provider may, upon proof of involvement, transmit data confirming the identity of the signatory or the person placing the seal, as well as data verified pursuant to section 85 to the party with opposing interests or his representative, and may disclose such data to the requesting court.

(4) If a relying party is indicated in a certificate under a pseudonym, the trust service provider may disclose data concerning the real identity of the relying party indicated in the certificate only with the consent of the relying party concerned, the trust service client, or another person represented by the relying party confirmed by the certificate, or in a situation specified in paragraphs (1) to (3).

Chapter XVIII

SUPERVISION OF TRUST SERVICES, AND PUBLICATION OF TRUSTED LISTS

48. Designation, tasks, and competence of the trust service supervisory body

Section 95 (1) The body supervising trust services pursuant to Article 46b (1) of the eIDAS Regulation shall be the National Media and Infocommunications Authority.

(2) The trust service supervisory body shall be responsible for publishing the trusted lists specified in Article 22 of the eIDAS Regulation.

Section 96 (1) In addition to the tasks provided for under the eIDAS Regulation, the trust service supervisory body shall

a) keep the registers specified in this Act and its implementing decrees, and publish registers in a manner that ensures they are continuously available to anyone;

b) monitor the development of technologies and cryptographic algorithms concerning trust services, and identify in its decisions the secure cryptographic algorithms trust service providers may use for their services, including requirements concerning the use of such algorithms with defined parameters;

c) with regard to trust services, perform the tasks of service supervisory body within the meaning of the Act on the general rules on taking up and pursuit of service activities.

(2) For the purposes of paragraph (1) b), a cryptographic algorithm shall be considered secure if it is not possible, using certain parameters, to deduct the data used to generate a signature or seal from the validation data of the given electronic signature or seal, and it also meets the conditions laid down in an implementing decree of this Act with regard to hashes.

Section 97 (1) The trust service supervisory body shall not conduct its proceedings as summary proceedings; the trust service supervisory body may invite a client more than one time to remedy any deficiency; the decision shall not be communicated orally.

(2) The Authority shall observe an administrative time limit of 2 months, unless provided otherwise by the eIDAS Regulation or its directly applicable Union implementing act.

(3) The Office of the National Media and Infocommunications Authority shall proceed as trust service supervisory body at first instance; appeals against its decisions shall be submitted to the President of the National Media and Infocommunications Authority.

(4) An administrative service fee, as specified in an implementing decree of this Act, shall be paid for the registration-related activities of the trust service supervisory body; such fees shall constitute revenue for the trust service supervisory body.

(5) The trust service supervisory body may, setting a time limit, prescribe a data provision obligation to the trust service providers pursuing activities falling within the scope of this Act, for the purpose of producing statistics, assessments, analyses, and evaluations as necessary to carry out its tasks specified in the eIDAS Regulation or referred to its competence. Trust service providers shall provide such data in full, accurately and in the form required by the trust service supervisory body, within the time limit set by the trust service supervisory body. If a data provider fails to meet this obligation, the trust service supervisory body may impose a fine as provided for under section 100.

(6) The trust service supervisory body shall inform the trust service provider providing the data about the processing and use of the data specified by the trust service supervisory body, as well as the purpose of data processing as defined by law, at the time of imposing the data provision obligation or requesting non-mandatory data provision. If data provision is ordered by way of a binding decision under paragraph (5), the trust service supervisory body shall inform the data provider about the legal consequences of any failure to provide, within the time limit, accurate data, in full and in the appropriate form; otherwise, the request shall indicate that data provision is not mandatory.

(7) The trust service supervisory body shall check, by means of an administrative audit conducted during the period of trust service provision, whether a natural person acting as qualified trust service provider, or an executive officer, manager, or employee of a legal person, or of an organisation without a legal personality, acting as qualified trust service provider has a criminal record or is subject to disqualification from a profession, excluding him from providing trust services. For the purposes of conducting administrative audits, the trust service supervisory body may request data from the criminal records system. Such data requests shall be limited to data indicating whether a natural person acting as a qualified trust service provider, or an executive officer, manager, or employee of a legal person, or of an organisation without a legal personality, acting as a qualified trust service provider has a criminal record or is subject to disqualification from a profession, excluding him from providing trust services.

(8) The trust service supervisory body shall process the personal data accessed under paragraph (7) until the discontinuation of the trust service provision activity or, where the qualified trust service provider is a legal person or an organisation without a legal personality, until the termination of the legal relationship between the organisation and its executive officer, manager, or employee.

(9) A client shall not request the trust service supervisory body to conduct an administrative audit. In the course of conducting an administrative audit *ex officio*, the trust service supervisory body shall proceed pursuant to section 99.

49. Registers relating to trust services

Section 98 (1) In addition to the provisions of the eIDAS Regulation, the trust service supervisory body shall also keep a register of the following:

a) notified trust service providers and trust services provided by them;

b) notified qualified electronic signature and qualified electronic seal creation devices;

c) designated organisations certifying the suitability of devices referred to in point b);

d) substitute trust service providers within the meaning of sections 92 and 93; and

e)

(2) The name, address, seat, and registration number of a trust service provider, the description of its service, the place and commencement date of service provision, and the trust service policy, service policy, service extract, and standard contract terms may be published in a register referred to in paragraph (1) as public data or documents. A register published by the trust service supervisory body shall be considered a publicly certified register, except for the name, address and seat of the trust service provider.

50. Audits conducted at trust service providers, and legal consequences available to the trust service supervisory body

Section 99 (1)

(2) At least once per year, the trust service supervisory body shall carry out a comprehensive on-site audit at trust service providers that provide qualified trust services. To obtain a statement by a specialist authority, the trust service supervisory body shall send to the competent authority the conformity assessment report prepared for the annual on-site audit in accordance with Article 20 (1) of the eIDAS Regulation.

(3) On the basis of facts and evidence discovered during an audit, and in order to ensure compliance with applicable requirements and to eliminate infringements and deficiencies, the trust service supervisory body

a) may apply, as measures, the following legal consequences:

aa) instructing, setting a time limit, a trust service provider to comply with applicable trust service requirements;

ab) prohibiting the use of specific measures and procedures;

ac) ordering, for a set period, the suspension of the provision of a service aimed at issuing new certificates, and publishing a reference to the suspension in the register;

b) may apply the following administrative sanctions:

ba) ordering the revocation of any qualified certificate issued previously;

bb) imposing an administrative fine;

bc) in a situation specified in the eIDAS Regulation, deleting a reference to a given trust service being a qualified trust service in respect of a trust service provided by a trust service provider;

bd) removing a trust service provider from the register of trust service providers.

(4) For a qualified trust service, the trust service supervisory body may, in addition to the situations specified in paragraph (3), take any measure and apply any legal consequence specified in paragraph (3) also in order to prevent any infringement or deficiency concerning an applicable requirement.

(5) The trust service supervisory body shall determine the measures and legal consequences referred to under paragraph (3) taking into account the gravity, frequency, recurrence, continuity, and duration of the infringement, the material gain obtained through the infringement, the harm to interests caused by the infringement, the number of persons who suffered or were exposed to harm to interests, the damage caused by the infringement, any violation of personality rights, and the impact of the infringement on the market, as well as any other considerations relevant to the specific case. Where the infringement is of minor gravity and no recurrence can be established, the trust service supervisory body may, establishing the infringement and setting an appropriate time limit, request the infringer to cease the infringing conduct, to refrain from future infringements, and to act in a lawful manner, and may set the requirements for doing so. The specific legal consequences and measures may also be applied jointly. In a proceeding of the trust service supervisory body, warning within the meaning of Act CXXV of 2017 on the sanctions for administrative violations shall not be applied.

(6) The trust service supervisory body shall deregister a trust service provider if compliance with the applicable trust service requirements cannot be ensured by any other means. Deregistration may be applied only if other measures fail to be effective.

(7) If a measure or legal consequence specified in paragraph (3) b) bc) or bd) is applied to a trust service provider that issues qualified certificates, the trust service supervisory body shall, at the same time, prohibit the trust service provider from referring to certificates issued by it as qualified certificates, and shall make arrangements for the revocation of any qualified certificate already issued.

(8) The trust service supervisory body may order a qualified certificate to be revoked if it seems likely that the qualified certificate includes any incorrect data, has been falsified, or that the device used by the trust service provider to sign or seal qualified certificates is not secure.

(9) If the trust service supervisory body prohibits the provision of a trust service, the trust service provider shall be obliged to proceed pursuant to section 92; if the trust service provider fails to fulfil this obligation, the trust service supervisory body shall proceed pursuant to section 93.

51. The amount of a fine imposed by the trust service supervisory body

Section 100 (1) The trust service supervisory body may impose a fine on a trust service provider that fails to meet the applicable trust service requirements.

(2) In the event of a recurring infringement, or if a trust service provider fails to comply with a decision by the trust service supervisory body, the trust service supervisory body may also impose a fine on the executive officer of the trust service provider, in addition to any fine imposed on the trust service provider.

(3) The trust service supervisory body shall not impose a fine if more than 2 years passed after the trust service supervisory body became aware of the infringement, or more than 3 years passed after the infringement was committed. If an omission or a breach of obligation constitutes a criminal offence, the trust service supervisory fine may be imposed within 1 year after the perpetration of the criminal offence is established with final and binding effect.

(4)

(5) The amount of the fine shall range

a) where the trust service provider is a natural person, from two hundred thousand forint to two billion forint;

b) where the trust service provider is a legal person, from one million forint to two billion forint or up to 1 per cent of the total global turnover of the undertaking to which the trust service provider belongs in the preceding financial year, if this amount exceeds two billion forint.

(6)

(7)

Chapter XIX

SPECIAL PROVISIONS ON CERTAIN TRUST SERVICES

52. Special provisions on trust services relating to electronic signatures and seals

Section 101 (1) If an electronic document is signed or sealed with a qualified electronic signature or seal, or a timestamp, the content of the document shall be presumed not to have changed since it was signed or sealed or the timestamp was applied, unless the verification of the signature, seal, or timestamp indicates otherwise.

(2) The certificate subject may use any data used to generate an electronic signature or seal for the sole purpose of generating electronic signatures and seals; other limitations indicated in the certificate shall also be observed, if any.

(3) A qualified electronic signature or seal certificate may also be used to generate advanced electronic signatures and seals.

(4) If any data used to generate electronic signatures or seals becomes known to an unauthorised person, or is lost, the trust service client shall notify the trust service provider without delay.

(5) If a trust service provider learns that any data used to generate electronic signatures or seals became known to an unauthorised person or is lost, it shall revoke the certificate, and publish a reference to the revocation in its register without delay.

(6) If a trust service provider learns that any data used to generate electronic signatures or seals may have become known, or is at risk of becoming known, to an unauthorised person, or such data has likely been lost, it shall suspend the certificate, and publish a reference to the suspension in its register without delay, provided that the trust service provider allows the suspension of the certificate.

Section 102 A fine under section 100 (5) may also be imposed if a trust service provider that provides a trust service relating to electronic signatures or seals fails to take measures, as necessary, to protect its own data used to generate electronic signatures or seals.

Section 103 (1) In the context of legal relationships regulated by family law or the law of succession, electronic signatures or seals may not be used and electronic documents bearing an electronic signature or seal may not be generated in an exclusive manner, without relying on documents in non-electronic formats.

(2) Unless provided otherwise explicitly, any reference in a law to electronic signatures or documents signed by electronic means shall be construed as referring to electronic seals or documents bearing an electronic seal as well.

53.

Section 104

Chapter XX

SPECIFIC SERVICES RELATING TO TRUST SERVICES, NOT QUALIFYING AS TRUST SERVICES

54. Role certification

Section 105 The role of a natural person certificate subject (for the purposes of this subtitle, hereinafter the “subject”) may be certified by means of a role certificate by the role certification provider designated in a decree of the Government decree. As a role certification provider the Government shall designate a government authentication service provider.

Section 106 (1) Where a role certificate is used, the role certification provider shall have the right, upon an electronic request for certification of a role from the subject, to process, and to receive from the role register, the personal data necessary for identifying the subject and certifying the role, for the period required to issue the role certificate. The service provider shall physically and logically separate the data relating to the role certificate.

(2) The organ keeping the role register shall ensure the provision of the data referred to in paragraph (1) with the assistance of the role certification provider.

Section 107 (1) With a view to ensuring the uniform use of role certificates, the Government shall provide a role certification platform service as a central electronic administration service.

(2) The role certification provider shall provide the subject with a role certificate through the role certification platform service.

(3) The provider of the role certification platform service shall have the right to process the personal data necessary for identifying the subject, and for selecting the service provider, for the period required to issue the role certificate. The service provider shall physically and logically separate the data relating to the role certificate.

PART SEVEN

FURTHER PROVISIONS RELATING TO THE DIGITAL STATE

55. Public services provided for organs performing a public duty that do not fall under the direction or supervision of the Government

Section 108 (1) The central service provider designated in the government decree on centralised IT and electronic communications services, and the government communications service provider designated in the government decree on government networks (hereinafter jointly the "central service provider") shall provide the following as public services to organs performing a public duty that do not fall under the direction or supervision of the Government:

a) development and operation, or contribution to the development, of the IT system specified in a decree by the minister responsible for e-governance;

b) centralised IT and communications services specified in the government decree on centralised IT and electronic communications services;

c) use of government networks specified in the government decree on government networks, as well as government communications activities, and government communications services,

provided that the head of the organ performing a public duty that does not fall under the direction or supervision of the Government applies to the minister responsible for e-governance for the use of such services.

(2) Funds for the use of the services referred to in paragraph (1) and for the provision of public services by the central service provider shall be provided for, depending on the outcome of negotiations between the minister responsible for e-governance and the head of the organ performing a public duty that does not fall under the direction or supervision of the Government,

a) in the budget of the ministry headed by the minister responsible for e-governance, directly or by way of transfer from the budget of the organ performing a public duty that does not fall under the direction or supervision of the Government; or

b) by the organ performing a public duty that does not fall under the direction or supervision of the Government if it enters into a contract with the central service provider directly.

(3) By way of derogation from paragraph (1), the IT central service provider for policing designated in a decree of the Government shall provide, as public services, the public services specified in the government decree on the provision of IT public services for policing to organs performing a public duty that do not fall under the direction or supervision of the Government, provided that the head of the organ performing a public duty that does not fall under the direction or supervision of the Government applies to the minister responsible for policing for the use of such services.

(4) By way of derogation from paragraph (2), funding for the use of services referred to in paragraph (3), and for the provision of public services by the central service provider, shall be provided for, depending on the outcome of negotiations between the minister responsible for policing and the head of the organ performing a public duty that does not fall under the direction or supervision of the Government,

a) in the budget of the ministry headed by the minister responsible for policing, directly or by way of a transfer from the budget of the organ performing a public duty that does not fall under the direction or supervision of the Government; or

b) by the organ performing a public duty that does not fall under the direction or supervision of the Government if it enters into a contract with the central service provider directly.

(5) If the Government does not designate a IT central service provider for policing, the Government shall ensure the performance of the tasks referred to in paragraphs (3) and (4) as provided for in paragraphs (1) and (2).

56. Electronic deeds in civil law relationships

Section 109 (1) Unless otherwise provided by law, an electronic private deed means an electronic document authenticated by the party making a statement, by means of the signature specified in section 8, point 23 and an electronic time stamp, or the service *eAláírás* (eSignature). A juridical act made as an electronic private deed shall qualify as written also within the meaning of section 6:7 (2) and (3) of Act V of 2013 on the Civil Code.

(2) Unless otherwise provided by law, in the context of real estate, law of succession, family law, companies, and non-governmental organisations, an electronic private deed shall qualify as written only if it contains a juridical act recorded exclusively in text form.

(3) By way of derogation from paragraph (1), an electronic document containing a juridical act in relation to a service provided by organisations and persons falling with the scope of the Acts listed in section 39 (1) of Act CXXXIX of 2013 on the Hungarian National Bank (for the purpose of this subtitle, hereinafter the "organisation") shall also qualify as an electronic private deed, provided that it was signed by means of a simple electronic signature suitable also for ascertaining the time of signature by the party making the statement, whom the organisation identified by an audited means of electronic communications or an electronic client-identification and statement-submission system specified in a decree issued on the basis of authorisation by section 77 (3) d) of Act LIII of 2017 on the prevention and combating of money laundering and terrorism financing (for the purposes of this subtitle, hereinafter "electronic identification").

(4) The electronic private deed referred to in paragraph (3) shall qualify as a private deed of full probative value.

(5) By way of derogation from paragraph (3), in the context of a contract for a service provided by the organisation, its amendment, and termination, an electronic private deed shall qualify as written only if it contains a juridical act recorded exclusively in text form.

(6) For the purpose of this section, a juridical act recorded in an electronic form, in particular as text or as sound, image or audio-visual recording, shall qualify as an electronic document.

Section 110 (1) In the event of a court or authority proceeding, the organisation shall be required to provide the court, or the authority, and the parties to the action affected by the juridical act, with the electronic private deed referred to in section 109 (3).

(2) In the event of a failure to comply with the provisions of paragraph (1), any statement of fact made by the party entering into a contract with the organisation (hereinafter the "party") relating to the juridical act recorded in the electronic private deed shall be presumed to be true.

(3) A juridical act may be drawn up as an electronic private deed referred to in section 109 (3) only if the party gave express consent to using the technology before the electronic signature.

(4) If the juridical act is made before electronic identification, the organisation shall record the communication in full and the transferred data content, and provide it to the party upon request.

(5) Where the party qualifies as a consumer, the organisation shall be required to provide the party with a copy of the contract concluded following electronic identification.

57. Central address register

Section 111 (1) The central address register shall serve to improve the interoperability of registers that are kept by cooperating organs and contain address data, and to ensure the consistency of address management.

(2) The central address register shall constitute a central register that improves the interoperability of different registers, and that serves as an authentic data source of address data, through an information transmission service, for registers that are kept by cooperating organs and contain address data.

(3) The detailed procedural rules on keeping and operating the central address register, and managing addresses in a consistent manner, shall be laid down in a government decree adopted on the basis of authorisation by this Act.

(4) The detailed rules on generating addresses in a consistent manner shall be laid down in a government decree adopted on the basis of authorisation by this Act.

Section 112 (1) With a view to ensuring that entries are made into the address register only by persons authorised by law, and in full compliance with applicable legislation, the organ responsible for operating the central address register shall keep a register of persons authorised to record addresses (hereinafter the "access authorisation register"). For this purpose, the organ responsible for operating the central address register may process the natural identification data of registered persons.

(2) The access authorisation register shall contain the following:

a) natural identification data of the persons concerned;

b) the territory of competence of the organ responsible for generating addresses;

c) the commencement date, and period of, access authorisation; and

d) the reason for, and date of, any change to, or cancellation of, access authorisation.

(3) Data entered into the access authorisation register may be consulted only for the purposes of verifying access authorisation, and compliance with statutory provisions by a person with access authorisation.

(4) Data entered into the access authorisation register shall be deleted no later than 5 years after the termination of access authorisation.

(5) If any address data the determination of which falls within the competence of a local government representative body needs to be obtained for the purpose of generating a new address in, or modifying or deleting an existing address from, the central address register, the representative body shall pass the decision, as necessary for generating the address, at its next session held after receipt of the request from the organ responsible for operating the central address register, and it shall notify the organ responsible for operating the central address register accordingly without delay.

(6) Address data of public interest, or accessible on public interest grounds, that are recorded in the central address register may be accessed through state or local government registers connected to the central address register.

57/A. **Central storage of image, sound, and audio-visual recordings**

Section 112/A (1) The organ designated by the Government in a decree (hereinafter "storage provider") shall ensure, through an IT application, by operating a central storage, the storage of image, sound, and audio-visual recordings (hereinafter "recording") produced by the following:

a) road operators;

b) the police, in the context of traffic policing measures;

c) image recorders deployed by the police;

d) image recorders deployed by a public space supervision authority;

e) those pursuing personal and property protection activities for the protection of private areas open to public of financial service providers and supplementary financial service providers, that are necessary for their tasks;

f) service providers within the meaning of section 8 (1) of Act XLI of 2012 on passenger transport services;

g) toll collectors within the meaning of the Act on toll to be paid for using highways, motorways and main roads proportionate to the distance travelled (hereinafter jointly "mandatory central storage user").

(2) The storage provider shall ensure, through an IT application, by operating a central storage, the storage of data recorded by the service provider referred to in section 16/A e) of the Act on the local governments of Hungary.

(3) The activities of the storage provider shall be limited to storing recordings and data at its central storage, and to providing the IT application referred to in section 112/B; it may not access, or perform any data processing operation with, any recording or data stored at the central storage.

(4) Mandatory central storage users shall cooperate with the storage provider as required under a government decree, and, where the conditions laid down in the government decree are met, use the central storage.

(5) When using the central storage, mandatory central storage users shall comply with the conditions laid down in the government decree referred to in paragraph (4).

Section 112/B (1) Where the police, a national security service, a professional disaster management organ, and, in a criminal proceeding, the court, the prosecution service, an investigating authority, or an organ conducting preparatory proceedings (hereinafter jointly "authorised data recipient") is authorised to receive any recording or data produced by a mandatory central storage user as laid down in an Act, the mandatory central storage user shall, if it uses the central storage, ensure the transfer of the data using the IT application operated by the storage provider.

(2) No recording or data produced by a mandatory central storage user shall be requested from the storage provider; to the transmission of such data, the data transmission rules laid down in the applicable sectoral Act shall apply.

Section 112/C (1) A register of mandatory central storage users and authorised data recipients shall be kept for the purpose of storing data of the storage provider, the mandatory central storage users, and the authorised data recipients, that are required for access, and of ensuring the verification of the lawfulness of data processing.

(2) The register of mandatory central storage users and authorised data recipients shall contain the following data concerning mandatory central storage users and authorised data recipients:

a) name;

b) postal address;

c) phone number;

d) fax number;

e) electronic mail address;

f) type of access authorisation, and a reference to the fact, and the date, of granting and cancelling the access authorisation;

g) with regard to any person holding access authorisation on behalf of an organisation (hereinafter the "person holding access authorisation"):

ga) family and given name;

gb) position;

gc) organisational unit;

gd) scope and extent of access authorisation, and a reference to the fact, and the date, of granting or cancelling the access authorisation;

ge) unique identifier.

Section 112/D (1) Unique identifiers, that are necessary for recording data in the central storage and accessing data stored in the central storage by electronic means, using an IT application, shall be requested by mandatory central storage users and authorised data recipients by means of submitting an application to the storage provider (hereinafter "application for unique identifier").

(2) An application for unique identifier shall contain all data specified in section 112/C (2) a) to f) and g) ga) to gd).

(3) Mandatory central storage users and authorised data recipients shall notify the storage provider of any change to the data referred to in paragraph (2) within three working days of the change.

(4) Within eight days of receipt of an application for unique identifier, the storage provider shall inform

a) a mandatory central storage user of the unique identifier of the person holding access authorisation, as well as the technical information required for using the central storage and the IT application;

b) an authorised data recipient of the unique identifier of the person holding access authorisation, as well as the technical information required for using the IT application.

(5) Recordings and data recorded in the central storage shall be processed only by electronic means, using an IT application.

Section 112/E (1) The storage provider shall keep a data access register for the purpose of verifying the lawfulness of data requests and data transfers from the central storage that are carried out by electronic means, using an IT application.

(2) The data access register shall contain the following:

a) identification data of the recording;

b) unique identifier of the person holding access authorisation;

c) date and time of data transfer;

d) provision of an Act, authorising the authorised data recipient to process the data in its proceeding, or in the course of pursuing its control activities or exercising its control functions;

e) designation of the data transferred.

(3) Data may be requested from the data access register by the following:

a) the National Authority for Data Protection and Freedom of Information;

b) the court, the prosecution service, an investigating authority, or an organ conducting preparatory proceedings, for the purposes of preventing and detecting criminal offences indicating the abuse of data, and conducting criminal proceedings;

c) a national security service and a law enforcement organ, for the purpose of performing their tasks set out in an Act.

57/B. European Digital Identity Wallet

Section 112/F (1) The Government shall make available, through the service provider designated in a decree of the Government, the national Member State European Digital Identity Wallet tool provided in accordance with the obligation set out in Articles 1 a) and 5a (1) of the eIDAS Regulation, and in line with the provisions set out in Article 5a of the eIDAS Regulation

(2) The Government shall designate in a decree the provider of person identification data, and of the electronic attestations of attributes issued on behalf of a public sector body, for the European Digital Identity Wallet

57/C Supervision of the European Digital Identity Wallet framework

Section 112/G (1) The authority that supervises the European Digital Identity Wallet framework referred to in Article 46a of the eIDAS Regulation shall be the National Media and Infocommunications Authority (hereinafter the "European Digital Identity Wallet supervisory authority").

(2) The European Digital Identity Wallet supervisory authority referred to in paragraph (1) shall carry out its tasks in accordance with the detailed rules set out in a decree of the Government.

(3) For authority proceedings by the European Digital Identity Wallet supervisory authority, administrative service fee shall be paid.

PART EIGHT

FINAL PROVISIONS

58. Authorising provisions

Section 113 (1) Authorisation shall be given to the Government to determine in a decree

1. the detailed rules of digital service use and provision, and electronic administration and communication;

2. the digital citizenship services and supporting services under this Act, and the detailed requirements for using and providing these services, as well as the organisational conditions for service provision, the personnel-related and financial conditions for service providers, and the provisions relating to the notification of the service;

3. the digital citizenship services and supporting services other than those specified in this Act, the detailed procedural rules of service provision, the detailed requirements for service use, the organisational conditions for regulated electronic administration service provision, the personnel-related and financial conditions for service providers, and the detailed rules relating to granting licence for a regulated electronic administration service;

4. the conditions for the use of a central state service provided to market participants by an organ other than an electronic administration organ, the tasks and procedure of the Authority in the course of such use, the method for determining the fee to be applied for such use of the service, the technical divergences of central state services provided to market participants, and the conditions for restricting the provision of central state services provided to market participants;

5. the detailed requirements for the identification of digital service providers;

6. the detailed rules concerning the methods of electronic communication;

7. the detailed rules of applying and registering administrative settings;

8. the special requirements concerning electronic signatures used for electronic administration, certificates relating to electronic signatures, and services relating to electronic signatures provided in connection with such purposes;

9. the detailed rules of operating the link register and providing data from the link register;

10. the detailed rules on electronic payments and settlements;

11. the detailed procedural rules of the Authority, the provisions relating to the imposition of fines and the amount of such fines;

12. the detailed rules on the registration of supporting service providers;

13. certain information provision obligations relating to digital service providers and digital citizenship service providers, the forms of information provision, the rules on performing these obligations by means of a national call centre (hereinafter the "call centre"), and the detailed rules on the operation of the call centre;

14. the detailed rules on producing electronic copies of paper-based documents, and converting electronic records into authentic paper-based records;

15. the procedure and frequency for backing up data concerning matters administered by digital service providers, as well as the organ responsible for safekeeping such data;

16. other identification methods recognised at national level which provide equivalent assurance in terms of reliability to physical presence;

17. the detailed rules relating to joining and operating the single digital gateway;

18. the sources of information to be used in the context of IT cooperation, the cooperating organs that are obliged to use automatic information transmission, the scope of information to be transferred in such a manner, and the requirements for information transmission services ensuring automated transfer;

19. the detailed procedural rules to be followed in case of any planned outage or malfunction;

20. the range of IT public services for policing, and the detailed rules on the provision of IT public services for policing;

21. the rules on keeping and operating the central address register and generating addresses in a consistent manner, as well as the detailed procedural rules for managing addresses in a consistent manner;

22. the roles, the detailed rules for role certification, together with the issuance of role certificates and the related liability rules, as well as the detailed rules relating to the role certification platform service;

23. the tasks of the digital service centre, and the requirements for designing and implementing services;

24. the cases in which no disadvantageous legal consequence may be applied to the user in the event of mandatory electronic administration;

25. the requirements concerning the content of the register kept by the trust service supervisory body, and the requirements concerning notifications relating to trust service provision;

26. the rules relating to the development, establishment and operation of the controlled environment referred to in Article 2, point (14) of Regulation (EU) 2024/903 of the European Parliament and of the Council, and to the connection to that environment;

27. the professional and infrastructural requirements for the integrator;

28. requirements relating to certifying organisations within the meaning of section 81 (4), certification, and the maximum fee, calculated without value added tax, of the certification procedure;

29. the manner in which the fulfilment of the conditions specified in section 81 (1) to (7) is to be continuously ensured, and in which it is to be certified.

(2) Authorisation shall be given to the Government to determine in a decree

1. the date referred to in section 7 (3);

2. the detailed rules of the activation and deactivation of a user profile, the application and registration of administrative settings, and the digital citizenship pre-registration;

3. the rules on designing and selecting roles, and ensuring related functions, using the user profile, and the rules applicable to the termination of the user profile;

4. the legal effects of the deactivated status of the user profile, and the conditions for reactivation;

5. the electronic document formats to be used through the service *ePosta* (ePost);

6. a reference to the regulated electronic administration service, or the regulated electronic administration service to be provided as a mandatory government service, to which the digital framework service corresponds, and to the regulated electronic administration service through which it can be ensured;

7. the types of electronic storage corresponding to the electronic registered delivery service, and the communication possibilities between them;

8. the specific functions of the national digital identity wallet service, and the conditions for providing and using the service;

9. the rules on electronic communication between organs required to provide a digital service, and between organs required to provide a digital service and natural persons or economic operators;

10. the proactive services, and the rules on the provision of proactive services;

11. the data registered by the digital citizenship service provider for the purpose of consent-based data provision;

12. the rules on aggregate service provision, connection to the service, expert services available in the course of connecting to and using the service, fees for such expert services, and keeping the register of connecting organs;

13. the detailed rules on the tasks of the European Digital Identity Wallet supervisory authority.

Section 114 (1) Authorisation shall be given to the Government to designate in a decree

1. the digital service centre;

2. the Authority;

3. the digital citizenship service provider;

4. the organ keeping the register of foreign nationals using electronic administration;

5. the providers of regulated electronic administration services provided as a mandatory government service, and the providers of central electronic administration services;

6. the organ keeping the digital citizenship register, and the registration organs of electronic identification services provided as a mandatory government service, and of the client settings register;

7. the organ operating the national call centre;

8. the operator of the electronic point of contact;

9. the IT central service provider for policing;

10. the organ responsible for operating the central address register;

11. the role certification provider;

12. the provider, and professional contributor, of a life-event-based service;

13. the framework application service provider;

14. the framework service provider;

15. the organ providing the system referred to in section 31 (1);

16. the storage provider;

17. the European Digital Identity Wallet provider;

18. the provider of person identification data, and of the electronic attestations of attributes issued on behalf of a public sector body, for the European Digital Identity Wallet.

(2) Authorisation shall be given to the Government to determine in a decree

1. the rules on the data processing referred to in section 15 (2) to (5);

2. the amount, and payment method, of the service fee to be paid to an organisation required to ensure a digital service for making available, within the framework of a data sharing service, any data and changes to data of users holding an activated user profile;

3. the amount, and payment method, of the service fee to be paid to the digital citizenship service provider by organisations required to ensure a digital service and organisations connecting voluntarily;

4. the conditions under section 9 (4a) for the use of a digital citizenship service or a supporting service by an organisation required to ensure a digital service or an organisation connecting voluntarily, and the further admission conditions;

5. the digital services in the life-event catalogue, their content and the related data processing matters, as well as the detailed rules on cooperation between the life-event service provider and the professional contributor;

6. the rules on consent-based data provision;

7. the requirements as regards the scope, and procedure, of the provision of the service *ePapír* (ePaper), as well as the detailed requirements for using the service;

8. the rules of cooperation between mandatory central storage users and the storage provider, and the rules of using the central storage;

9.the detailed rules on specific supporting services and expert services provided to third-party service providers in the course of their connection to and use of central state services provided to market participants, and on determining the relevant fees;

10. the detailed rules on expert services available to organisations required to ensure a digital service, and on determining the fees.

Section 115 (1) Authorisation shall be given to the minister responsible for e-governance to determine in a decree

1. the detailed requirements concerning trust services, including, in particular, requirements concerning the financial and personnel-related suitability and activities of, and devices used by, trust service providers, requirements for contracting with relying parties and for the information provision obligation in relation to contracting, and detailed conditions for service contracts and other conditions for providing trust services (such as trust service policies and service policies);

2. in agreement with the minister responsible for taxation policy, the amount of administrative service fee payable to the trust service supervisory body, and the European Digital Identity Wallet supervisory authority, as well as the detailed rules concerning the payment, management, registration, and reimbursement of any such fee;

3. the rules on using centralised IT and communications services by organs performing a public duty that do not fall under the direction or supervision of the Government, IT systems developed or operated by a central service provider, and government networks and network services;

4. in agreement with the minister responsible for taxation policy, the amount, and payment method, of the administrative service fee to be paid by organisations required to ensure a digital service, market participants other than an organisation required to ensure a digital service, and organisations connecting voluntarily;

5. in agreement with the minister responsible for taxation policy, the amount, and payment method, of the administrative service fee to be paid to an organisation required to ensure a digital service, a market participant other than an organisation required to ensure a digital service, and an organisation connecting voluntarily, for making available, within the framework of an aggregate service, any data, and changes to data, of users holding an activated user profile.

(2) Authorisation shall be given to the president of SARA to determine in a decree

a) the cybersecurity requirements for a regulated electronic administration service, and the manner for proving compliance with the requirements;

b) the detailed procedural rules on keeping the register of integrators; and the detailed rules on data, other than personal data, included in the register.

59. Provisions on entry into force

Section 116 (1) This Act shall enter into force on 1 July 2024, with the exceptions specified in paragraphs (2) and (3).

(2) Sections 18 to 24, sections 26 to 38, section 39 (2) c) to l), section 40, section 45, section 46 (1) b), section 46 (2) to (4) and (6) to (8), sections 47 to 51, sections 65 to 70, sections 72 to 79, sections 82 to 112, and section 121 shall enter into force on 1 September 2024.

(3) Part Five shall enter into force on 1 June 2025.

60. Transitional provisions

Section 117 (1) In matters pending before the Electronic Administration Supervisory Authority within the meaning Act CCXXII of 2015 on the general rules on electronic administration and trust services (hereinafter the "e-Administration Act") on 31 August 2024, the Authority shall proceed in accordance with the provisions of this Act.

(2) As of 1 September 2024, data processed within the functions of the Electronic Administration Supervisory Authority on 31 August 2024 shall be processed by the Authority.

Section 118 (1) From 1 July 2024 to 1 September 2024, the provisions of this Act shall apply, together with the provisions of the e-Administration Act, in a manner that they do not prejudice services to be mandatorily provided under the e-Administration Act, and legal effects arising under the e-Administration Act.

(2) Digital service providers other than the legal entities referred to in Part Five, shall be required to provide digital services in compliance with this Act from 1 July 2025.

(3) Until the time limit set in paragraph (2), electronic administration organs within the meaning of the e-Administration Act as in force on 31 August 2024 that operated, on 31 August 2024, an electronic information system within the meaning of the e-Administration Act as in force on 31 August 2024 shall

a) be entitled to ensure the administration of matters by electronic means through an electronic information system in accordance with the provisions in force on 31 August 2024 of the e-Administration Act as in force on 31 August 2024; and

b) ensure cooperation under the e-Administration Act in accordance with the provisions in force on 31 August 2024 of the e-Administration Act as in force on 31 August 2024.

(4) Legal entities qualifying as public utility service providers within the meaning of the provisions in force on 30 June 2024 of the e-Administration Act as in force on 31 August 2024 shall fulfil their obligations set out in the e-Administration Act as in force on 31 August 2024 and its implementing decrees in accordance with the provisions in force on 31 August 2024 of the e-Administration Act as in force on 31 August 2024 until the entry into force of Part Five of this Act.

(5) Following the entry into force of this Act, digital service providers may deploy new IT systems only if they are in compliance with this Act.

(6) Where enabled under the e-Administration Act as in force on 31 August 2024, a procedural act or statement requiring appearance in person of the user when using non-electronic administration may be performed or made, until the date set out in paragraph (2), by electronic means, if the user identifies himself by using electronic identification that can be traced back to the user having previously been identified in person in a manner enabling his identity to be unambiguously matched to his person.

Section 119 (1) The digital citizenship service provider shall provide the digital citizenship services under this Act from the following date at the latest:

a) framework application from 1 September 2024;

b) national digital identity wallet service from 1 September 2024;

c) consent-based data provision from 1 June 2025;

d) service *eAláírás* (eSignature) from 1 September 2024;

e) service *eAzonosítás* (eIdentification) from 1 September 2024;

f) service *ePosta* (ePost) from 1 January 2026;

g) service *eDokumentumkezelés* (eDocument management) from 1 January 2026;

h) service *eFizetés* (ePayment) from 1 January 2026.

(2) The use of the identification-based document authentication service under the e-Administration Act as in force on 31 August 2024 shall be enabled in the custom front office until 31 December 2024. From 1 January 2025, the identification-based document authentication service shall be provided only to digital service providers for the authentication of the statements of persons acting on behalf of the service provider and, until 31 October 2025, in an integrated manner with the supporting service.

(3) Until 31 December 2026, the client settings register shall ensure access to and the application of settings that it does not process and ensure under this Act, but that are recorded in the register of the administrative settings of the client in accordance with the e-Administration Act as in force on 31 August 2024 and are effective in relation to the requesting organ under the law, except for juridical acts relating to changing the method of electronic identification, the encryption of electronic documents, and requesting periodic notification concerning electronic administrative acts.

(4) A setting referred to in paragraph (3) may be applied until the first activation of the digital citizenship user profile in accordance with section 63. By way of derogation from paragraph (3), a person holding an active user profile shall not make a juridical act relating to changing the method of electronic identification, the encryption of electronic documents, or requesting periodic notification concerning electronic administrative acts.

(5) A person falling within the scope of the register of personal data and addresses who used an electronic identification service provided as a mandatory government service that was discontinued by this Act shall, by 15 January 2025, switch to using a service listed in section 46 (1) a) and b), at his discretion, for the administration of digital matters requiring identification. For the purposes of this paragraph, electronic identification services provided as a mandatory government service may continue to be used until the switch.

(6) By way of derogation from section 46 (3), a person falling within the scope of the register of personal data and addresses may, until 31 December 2028, identify himself using all electronic identification services provided as a mandatory government service referred to in section 46 (1).

(7) A natural person user who is recorded in the central aliens policing register, or the register of foreign nationals using electronic administration, may use the *ügyfélkapu* (Client Gate) until 14 January 2025, and the identification service referred to in section 46 (1) b) from 15 January 2025.

(8) From 1 September 2024, data required for generating an electronic signature shall not be placed on the storage component of the permanent identity card referred to in the Registration Act.

(9) Until 31 December 2026, the Government shall provide, as a regulated electronic administration service under section 45 (1) b), a secure delivery service recognised at national level, that does not qualify as a trust service, under the e-Administration Act as in force on 31 August 2024.

(10) Until 31 December 2025, the client settings register shall include only data referred to in section 13 (1) e) that are related to the regulated electronic administration service provided by the Government under section 45 (1) b).

(11) The digital citizenship service provider shall ensure the possibility of identification by means of remote identification as referred to in section 63 (1) a) aa) from 31 January 2025 at the latest.

Section 120 (1) From 1 July 2024, the Central Client Registration Records under the e-Administration Act as in force on 30 June 2024 shall form part of the digital citizenship register; for the Central Client Registration Records, all data processing and technical processing operations shall cease; all obligations relating to the Central Client Registration Records shall be fulfilled by the organ keeping the digital citizenship register.

(2)

(3) A person who has not attained the age of 14 and falls within the scope of the register of personal data and home addresses shall be entitled to a digital citizen identifier and a user profile under this Act from 15 February 2028.

61. Repealing provision

Section 121

62. Compliance with the law of the European Union

Section 122 (1) This Act contains provisions for the implementation of Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC and of Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No 910/2014 as regards establishing the European Digital Identity Framework amending it.

(2) This Act contains provisions to implement Regulation (EC) No. 223/2009 of the European Parliament and of the Council of 11 March 2009 on European statistics and repealing Regulation (EC. Euratom) No. 1101/2008 of the European Parliament and of the Council on the transmission of data subject to statistical confidentiality to the Statistical Office of the European Communities, Council Regulation (EC) No. 322/97 on Community Statistics, and Council Decision 89/382/EEC, Euratom establishing a Committee on the Statistical Programmes of the European Communities.

(3) This Act contains provisions for the implementation of Regulation (EU) 2018/1724 of the European Parliament and of the Council of 2 October 2018 establishing a single digital gateway to provide access to information, to procedures and to assistance and problem-solving services and amending Regulation (EU) No 1024/2012.

(4) This Act contains provisions for the implementation of Regulation (EU) 2024/903 of the European Parliament and of the Council of 13 March 2024 laying down measures for a high level of public sector interoperability across the Union (Interoperable Europe Act).

Section 123 (1) This Act serves the purpose of compliance with Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

(2) The draft of this Act was notified in advance pursuant to Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

(3) The draft of section 80 (1) o) was notified in advance pursuant to Articles 5 to 7 of Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.